

АКТУАЛЬНЫЕ ПРОБЛЕМЫ РОССИЙСКОГО ПРАВА

№ 6 (103) ИЮНЬ 2019

ТЕМА НОМЕРА

**ПРАВО
В УСЛОВИЯХ
ЦИФРОВИЗАЦИИ**

АКТУАЛЬНЫЕ ПРОБЛЕМЫ РОССИЙСКОГО ПРАВА



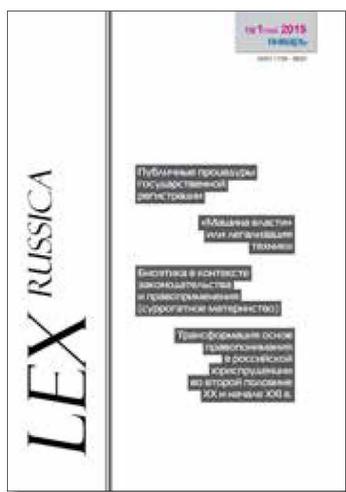
- ✓ Свидетельство о регистрации СМИ — ПИ № ФС77-25128 от 7 мая 2014 г., ISSN 1994-1471;
- ✓ издается с 2004 г., с 2013 г. — ежемесячно;
- ✓ входит в перечень ВАК России;
- ✓ включен в Российский индекс научного цитирования (РИНЦ) и Ulrich's Periodicals Directory;
- ✓ каждой статье присваивается индивидуальный международный индекс DOI;
- ✓ отдельные материалы размещаются в СПС «КонсультантПлюс» и «ГАРАНТ», электронной библиотеке «КиберЛенинка».

«Актуальные проблемы российского права» — это научно-практический юридический журнал, посвященный актуальным проблемам теории права, практике его применения, совершенствованию законодательства, а также проблемам юридического образования. Рубрики

журнала охватывают все основные отрасли права, учитывают весь спектр юридической проблематики, в том числе теории и истории государства и права, государственно-правовой, гражданско-правовой, уголовно-правовой, международно-правовой направленности. На страницах журнала размещаются экспертные заключения по знаковым судебным процессам, материалы конференций, рецензии на юридические новинки.

В журнале активно публикуются не только известные ученые и практики, но и молодые, начинающие ученые, студенты юридических вузов. Конечно, размещается большое количество материалов ведущих специалистов Университета имени О.Е. Кутафина (МГЮА), в том числе выполненных в рамках НИРов, грантов, активно публикуются победители различных конкурсов.

LEX RUSSICA (РУССКИЙ ЗАКОН)



- ✓ Свидетельство о регистрации СМИ — ПИ № ФС77-58927 от 5 августа 2014 г., ISSN 1729-5920;
- ✓ издается с 2004 г., с 2013 г. — ежемесячно;
- ✓ является преемником научных трудов ВЮЗИ-МЮИ-МГЮА, издаваемых с 1948 г.;
- ✓ входит в перечень ВАК России;
- ✓ включен в Российский индекс научного цитирования (РИНЦ) и Ulrich's Periodicals Directory;
- ✓ каждой статье присваивается индивидуальный международный индекс DOI;
- ✓ отдельные материалы размещаются в СПС «КонсультантПлюс» и «ГАРАНТ», электронной библиотеке «КиберЛенинка».

Lex Russica («Русский закон») — научный юридический журнал, посвященный фундаментальным проблемам теории государства и права (в том числе этноправа), совершенствования законодательства и повышения эффективности правоприменения, правовой культуры, юридического образования и методики преподавания правовых дисциплин, международного права, сравнительного правоведения и др.

Журнал знакомит с юридическими школами вузов России; публикует очерки об ученых, чьи имена золотыми буквами вписаны в историю юридической науки, обзоры конференций и круглых столов, проведенных в Университете имени О.Е. Кутафина (МГЮА) или с участием профессорско-преподавательского состава Университета в других российских и зарубежных научных центрах, рецензии на новые юридические издания; содействует сближению и гармонизации российского и зарубежного права.

Авторами журнала являются известные российские и зарубежные ученые-юристы (из Германии, Китая, Польши, Франции, Финляндии и др.).

АКТУАЛЬНЫЕ ПРОБЛЕМЫ

№ 6 (103) ИЮНЬ 2019

РОССИЙСКОГО ПРАВА

Ежемесячный научный журнал.
Издается как СМИ с 2006 г.

Председатель редакционного совета журнала

**ГРАЧЕВА
Елена
Юрьевна** доктор юридических наук, профессор, заведующий кафедрой финансового права, первый проректор Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), заслуженный юрист РФ, почетный работник высшего профессионального образования РФ, почетный работник науки и техники РФ.
Почтовый адрес: 125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9.

Заместитель председателя редакционного совета журнала

**ЕРШОВА
Инна
Владимировна** доктор юридических наук, профессор, заведующий кафедрой предпринимательского и корпоративного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), почетный работник высшего профессионального образования РФ, почетный работник юстиции России, заслуженный юрист РФ.
Почтовый адрес: 125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9.

Главный редактор журнала

**СИТНИК
Александр
Александрович** кандидат юридических наук, доцент кафедры финансового права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА).
Почтовый адрес: 125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9.

Ответственный секретарь

**СЕВРЮГИНА
Ольга
Александровна** эксперт отдела научно-издательской политики НИИ
Университета имени О.Е. Кутафина (МГЮА).

Члены редакционного совета журнала

**БЕКЯШЕВ
Дамир
Камильевич** доктор юридических наук, доцент, доцент кафедры международного права Московского государственного института международных отношений МИД России.
Почтовый адрес: 119454, Россия, г. Москва, проспект Вернадского, д. 76.

**БЕЛОВА
(ГАНЕВА)
Габриела** кандидат юридических наук, доцент, декан историко-правового факультета Юго-Западного университета имени Неофита Рильского (Болгария).
Почтовый адрес: 2700, Болгария, г. Благоевград, ул. Ивана Михайлова, д. 66.

**БОЛТИНОВА
Ольга
Викторовна** доктор юридических наук, профессор, заместитель заведующего кафедрой финансового права, ученый секретарь Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), почетный работник высшего профессионального образования РФ.
Почтовый адрес: 125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9.

**БРИНЧУК
Михаил
Михайлович** доктор юридических наук, профессор, заведующий сектором эколого-правовых исследований Института государства и права Российской академии наук.
Почтовый адрес: 119019, Россия, г. Москва, ул. Знаменка, д. 10.

**ВИННИЦКИЙ
Данил
Владимирович** доктор юридических наук, профессор, заведующий кафедрой финансового права Уральского государственного юридического университета, директор Института права БРИКС.
Почтовый адрес: 620137, Россия, г. Екатеринбург, ул. Комсомольская, д. 21.

**ВОСКОБИТОВА
Лидия
Алексеевна** доктор юридических наук, профессор, заведующий кафедрой уголовно-процессуального права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), почетный работник высшего профессионального образования РФ.
Почтовый адрес: 125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9.

**ГАЗЬЕ
Анн** доктор права, доцент Университета Paris Quest Nanterre La Défense (Франция).
Почтовый адрес: 92001, Франция, г. Нантер, авеню Републик, д. 200.

**ГОЛОВНЕНКОВ
Павел
Валерьевич** доктор права, ассессор права, главный научный сотрудник кафедры уголовного и, в частности, экономического уголовного права юридического факультета Потсдамского университета (Германия).
Почтовый адрес: 14482, Германия, г. Потсдам, ул. Августа Бебеля, д. 89.



- ДУБРОВИНА Елена Павловна** кандидат юридических наук, член Центризбиркома России, заслуженный юрист РФ. Почтовый адрес: 109012, Россия, г. Москва, Б. Черкасский пер., д. 9.
- ЗАНКОВСКИЙ Сергей Сергеевич** доктор юридических наук, профессор, и. о. заведующего сектором предпринимательского и корпоративного права, главный научный сотрудник Института государства и права Российской академии наук. Почтовый адрес: 119019, Россия, г. Москва, ул. Знаменка, д. 10.
- ЗАХАРОВ Владимир Викторович** доктор юридических наук, профессор, председатель Арбитражного суда Курской области. Почтовый адрес: 305000, Россия, г. Курск, ул. Радищева, д. 33.
- КАЛИНИЧЕНКО Пауль Алексеевич** доктор юридических наук, профессор, профессор кафедры интеграционного и европейского права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА). Почтовый адрес: 125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9.
- КОКОТОВ Александр Николоевич** доктор юридических наук, профессор, судья Конституционного Суда РФ, заслуженный юрист РФ, почетный работник высшего профессионального образования РФ. Почтовый адрес: 190000, Россия, г. Санкт-Петербург, Сенатская пл., д. 1.
- КОРНЕВ Аркадий Владимирович** доктор юридических наук, профессор, заведующий кафедрой теории государства и права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА). Почтовый адрес: 125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9.
- КУРБАНОВ Рашад Афатович** доктор юридических наук, профессор, заведующий кафедрой гражданско-правовых дисциплин Российского экономического университета имени Г. В. Плеханова. Почтовый адрес: 117997, Россия, г. Москва, Стремянный пер., д. 36.
- ЛИПСКИ Станислав Анджеевич** доктор экономических наук, доцент, заведующий кафедрой земельного права Государственного университета по землеустройству. Почтовый адрес: 105064, Россия, г. Москва, ул. Казакова, д. 15.
- МАРИНО Иван** кандидат юридических наук, доцент Государственного университета «Ориентале» (Неаполь), руководитель Центра мониторинга политико-правовой системы России, Итальянского представительства Фонда конституционных реформ. Почтовый адрес: 80121, Италия, г. Неаполь, виа Карло Поэрио, д. 15.
- МАЦКЕВИЧ Игорь Михайлович** доктор юридических наук, профессор, заведующий кафедрой криминологии и уголовно-исполнительного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), президент Союза криминалистов и криминологов, заслуженный деятель науки РФ, почетный работник высшего профессионального образования РФ, заместитель председателя Экспертного совета Высшей аттестационной комиссии Минобрнауки РФ. Почтовый адрес: 125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9.
- ПАНАГИОТОПОЛОС Димитриос** доктор права, магистр философии, профессор Афинского университета, вице-ректор Университета Центральной Греции, президент Международной ассоциации спортивного права (IASL), специальный эксперт в области спортивного права в Европейском Союзе, награжден премией «Право: Человек года» (2009) Американским биографическим институтом (ИНК). Почтовый адрес: 10677, Греция, г. Афины, ул. Веранжероу, д. 4.
- ПЕТРОВА Татьяна Владиславовна** доктор юридических наук, профессор кафедры экологического и земельного права Юридического факультета Московского государственного университета имени М.В. Ломоносова. Почтовый адрес: 119991, Россия, ГСП-1, г. Москва, Ленинские горы, д. 1, стр. 13.
- РЕШЕТНИКОВА Ирина Валентиновна** доктор юридических наук, профессор, председатель Арбитражного суда Уральского округа, заслуженный юрист РФ, почетный работник судебной системы. Почтовый адрес: 620075, Россия, г. Екатеринбург, пр-т Ленина, д. 32/27.
- РОССИНСКАЯ Елена Рафаиловна** доктор юридических наук, профессор, заведующий кафедрой судебных экспертиз, директор Института судебных экспертиз Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), президент Ассоциации образовательных учреждений «Судебная экспертиза», академик РАЕН, заслуженный деятель науки РФ, почетный работник высшего профессионального образования РФ. Почтовый адрес: 125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9.

- СОКОЛОВ Александр Юрьевич** доктор юридических наук, профессор, заведующий кафедрой административного и муниципального права Саратовской государственной юридической академии. Почтовый адрес: 410056, Россия, г. Саратов, ул. Вольская, д. 1.
- ФОКИНА Марина Анатольевна** доктор юридических наук, профессор, профессор кафедры гражданского и административного судопроизводства Российского государственного университета правосудия. Почтовый адрес: 117418, Россия, г. Москва, ул. Новочеремушкинская, д. 69.
- ХВАН Леонид Борисович** кандидат юридических наук, доцент кафедры административного и финансового права Ташкентского государственного юридического института. Почтовый адрес: 100000, Республика Узбекистан, г. Ташкент, Главпочтамт, а/я № 4553.
- ЧАННОВ Сергей Евгеньевич** доктор юридических наук, профессор, заведующий кафедрой служебного и трудового права Поволжского института управления имени П.А. Столыпина. Почтовый адрес: 410031, Россия, г. Саратов, ул. Соборная, д. 23/25.
- ЧЕРНЫШЕВА Ольга Сергеевна** кандидат юридических наук, начальник отдела Секретариата Европейского Суда по правам человека. Почтовый адрес: 67075, Франция, г. Страсбург, Cedex, ЕСПЧ.
- ШАЛУМОВ Михаил Славович** доктор юридических наук, профессор, заместитель начальника управления систематизации законодательства и анализа судебной практики Верховного Суда Российской Федерации — начальник отдела систематизации законодательства и анализа судебной практики в области уголовного судопроизводства, судья Верховного Суда Российской Федерации (в почетной отставке).
- ШИТКИНА Ирина Сергеевна** доктор юридических наук, профессор, профессор кафедры предпринимательского права, руководитель программы магистратуры по направлению «Корпоративное право» Юридического факультета Московского государственного университета имени М.В. Ломоносова. Почтовый адрес: 119991, Россия, ГСП-1, г. Москва, Ленинские горы, д. 1, стр. 13.
- ЯСКЕРНЯ Ежи** доктор юридических наук, профессор, директор Института права, экономики и управления Университета имени Яна Кохановского в г. Кельц (Польша). Почтовый адрес: 25369, Польша, г. Кельц, ул. Зеромского, д. 5.
- Редакционная коллегия журнала*
- КАШАНИНА Татьяна Васильевна** профессор кафедры теории государства и права, доктор юридических наук, профессор. Почтовый адрес: 125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9.
- КЛЕПИЦКИЙ Иван Анатольевич** профессор кафедры уголовного права, доктор юридических наук, профессор. Почтовый адрес: 125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9.
- МИХАЙЛОВ Сергей Михайлович** и. о. заведующего кафедрой гражданского и административного судопроизводства, кандидат юридических наук, доцент. Почтовый адрес: 125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9.
- ОСАВЕЛЮК Алексей Михайлович** профессор кафедры конституционного и муниципального права, доктор юридических наук, профессор. Почтовый адрес: 125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9.
- ПОДУЗОВА Екатерина Борисовна** доцент кафедры гражданского права, кандидат юридических наук. Почтовый адрес: 125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9.
- СОКОЛОВА Наталья Александровна** заведующий кафедрой международного права, доктор юридических наук, доцент. Почтовый адрес: 125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9.

Chairperson of the Board of Editors

**GRACHEVA
Elena
Yurievna**

Doctor of Law, Professor, Head of the Department of Financial Law, First Vice-Rector of the Kutafin Moscow State Law University, Honored Lawyer of the Russian Federation, Honored Worker of Higher Professional Education of the Russian Federation, Honored Worker of Science and Technology of the Russian Federation.
Mailing address: 125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9.

Vice-Chairperson of the Board of Editors

**ERSHOVA
Inna
Vladimirovna**

Doctor of Law, Professor, Head of the Department of Business and Corporate Law of the Kutafin Moscow State Law University, Honored Worker of the Higher Professional Education of the Russian Federation, Honored Worker of Justice of Russia, Honored Lawyer of the Russian Federation.
Mailing address: 125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9.

Chief editor of the magazine

**SITNIK
Aleksandr
Aleksandrovich**

PhD in Law, Associate Professor of the Department of Financial Law of the Kutafin Moscow State Law University.
Mailing address: 125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9.

Executive Editor

**SEVRYUGINA
Olga
Aleksandrovna**

Expert of the Research and Publishing Policy Department of the Research Institute of the Kutafin Moscow State Law University (MSAL).

Members of the Board of Editors

**BEKYASHEV
Damir
Kamilievich**

Doctor of Law, Associate Professor, Associate Professor of the Department of International Law of Moscow State Institute of International Relations under the Ministry of Foreign Affairs of Russia.
Mailing address: 119454, Russia, Moscow, prospekt Vernadskogo, d. 76.

**BELOVA-GANEVA
Gabriela**

PhD in Law, Associate Professor, Dean of the Faculty of Law and History of the South Western University named after the Neophyte Rilsky (Bulgaria)
Mailing address: 2700, Bulgaria, Blagoevgrad, ul. Ivana Mikhailova, d. 66.

**BOLTINOVA
Olga
Viktorovna**

Doctor of Law, Professor, Vice-Chairperson of the Department of Financial Law, Academic Secretary of the Kutafin Moscow State Law University, Honored Worker of Higher Professional Education of the Russian Federation.
Mailing address: 125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9.

**BRINCHUK
Mikhail
Mikhailovich**

Doctor of Law, Professor, Head of the Sector for Environmental and Legal Studies of the Institute of State and Law of the Russian Academy of Sciences.
Mailing address: 119019, Russia, Moscow, ul. Znamenka, d. 10.

**CHANNOV
Sergey
Evgenievich**

Doctor of Law, Professor, Head of the Department of Service and Labor Law of the Povolzhsky Institute of Government named after P.A. Stolypin.
Mailing address: 410031, Russia, Saratov, Sobornaya ul., d. 23/25.

**CHERNISHOVA
Olga
Sergeevna**

PhD in Law, Head of Division at the Registry of the European Court of Human Rights.
Mailing address: European Court of Human Rights, 67075 Strasbourg Cedex, France.

**DUBROVINA
Elena
Pavlovna**

PhD in Law, Member of the Election Committee of Russia, Honored Lawyer of the Russian Federation.
Mailing address: 109012, Russia, Moscow, B. Cherkasskiy per., d. 9.

- FOKINA
Marina
Anatolievna** Doctor of Law, Professor, Professor of the Department of Civil and Administrative Proceedings of the Russian State University of Justice.
Mailing address: 117418, Russia, Moscow, ul. Novocheremushkinskaya, d. 69.
- GAZIER
Anne** Doctor of Law, Associate Professor of the University Paris Quest Nanterre La Défense (France).
Mailing address: Université Paris Ouest Nanterre La Défense, 200 avenue de la République, 92001, Quest Nanterre, La Défense, France.
- JASKIERNIA
Jerzy** Prof. dr hab. Jan Kochnowski University, Kielce, Poland, Department of Management and Administration Director, Institute of Economy and Administration, Chair, Administration and Legal Sciences Division.
Mailing address: Str. Żeromskiego 5, Kielce, Poland, 25369.
- KALINICHENKO
Paul
Alekseevich** Doctor of Law, Professor, Professor of the Department of Integration and European Law of the Kutafin Moscow State Law University.
Mailing address: 125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9.
- KHVAN
Leonid
Borisovich** PhD in Law, Associate Professor of the Department of Administrative and Financial Law of the Tashkent State Legal Institute.
Mailing address: 100000, Republic of Uzbekistan, Tashkent, Glavpochtamt, a/ya 4553.
- KOKOTOV
Aleksandr
Nikolaevich** Doctor of Law, Professor, Judge of the Constitutional Court of the Russian Federation, Honored Lawyer of the Russian Federation, Honored Worker of Higher Professional Education of the Russian Federation.
Mailing address: 190000, Russia, St. Petersburg, Senatskaya pl., d. 1.
- KORNEV
Arkadiy
Vladimirovich** Doctor of Law, Professor, Head of the Department of Theory of the State and Law of the Kutafin Moscow State Law University.
Mailing address: 125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9.
- KURBANOV
Rashad
Afatovich** Doctor of Law, Professor, Head of the Department of Civil Law Disciplines of the Plekhanov Russian Economic University.
Mailing address: 117997, Russia, Moscow, per. Stremyanny, d. 36.
- LIPSKI
Stanislav
Andjeevich** Doctor of Economics, Associate Professor, Head of the Department of Land Law of the State University for Land Use Planning.
Mailing address: 105064, Russia, Moscow, ul. Kazakova, d. 15.
- MARINO
Ivan** PhD in Law, Associate Professor of the University «L'Orientale», Head of the Monitoring Center for the Political and Legal System of Russia, and of the Italian Representative Office of the Constitutional Reforms Foundation.
Mailing address: via Carlo Poerio, 15, 80121, Napoli, Italia.
- MATSKEVICH
Igor
Mikhailovich** Doctor of Law, Professor, Head of the Department of Criminology and Penal Law of the Kutafin Moscow State Law University, President of the Union of Criminalists and Criminologists, Honored Scholar of the Russian Federation, Honored Worker of Higher Professional Education of the Russian Federation, Vice-chairman of Advisory Council of the Higher Attestation Commission of the Ministry of Education and Science of the Russian Federation.
Mailing address: 125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9.
- PANAGIOTOPOULOS
Dimitrios** Professor of University of Athens, Attorney-at-Law Vice-Rector, University of Central Greece, President of International Association of Sports Law (IASL), awarded «Person of the Year in Law» (2009) from the American Biographical Institute (INC).
Mailing address: 4 Veranzerou Str., 10677, Athens, Greece.
- PETROVA
Tatiana
Vladislavovna** Doctor of Law, Professor, Professor of the Department of Environmental and Land Law of the Faculty of Law of the Lomonosov Moscow State University.
Mailing address: 119991, Russia, GSP-1, Moscow, Leninskie Gory, d. 1, build. 13.
- RESHETNIKOVA
Irina
Valentinovna** Doctor of Law, Professor, Chairperson of the Arbitration Court of the Urals District, Honored Lawyer of the Russian Federation, Honored Worker of the Judicial System.
Mailing address: 620075, Russia, Ekaterinburg, prosp. Lenina, d. 32/27.



- ROSSINSKAYA
Elena
Rafailovna** Doctor of Law, Professor, Head of the Department of Forensic Examination of the Kutafin Moscow State Law University, President of the Association of Educational Institutions «Forensic Examination», Academician of the Russian Academy of Natural Sciences, Honored Scholar of the Russian Federation, Honored Worker of Higher Education of the Russian Federation.
Mailing address: 125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9.
- SHALUMOV
Mikhail
Slavovich** Doctor of Law, Professor, Deputy Head of Directorate — Chief of Branch of the Systematization of Legislation and Analysis of the Judicial Practice at Criminal procedure of the Directorate of the Systematization of Legislation and Analysis of the Judicial Practice of the Supreme Court of the Russian Federation, Justice of the Supreme Court of the Russian Federation (emeritus).
Mailing address: 121260, Russia, Moscow, ul. Povarskaya, d. 15.
- SHITKINA
Irina
Sergeevna** Doctor of Law, Professor, Professor of the Department of Business Law, Head of the «Corporate Law» Master's Program of the Law Faculty of the Lomonosov Moscow State University.
Mailing address: 119991, Russia, GSP-1, Moscow, Leninskie Gory, d. 1, build. 13.
- SOKOLOV
Aleksandr
Yurievich** Doctor of Law, Professor, Head of the Department of Administrative and Municipal Law of the Saratov State Law Academy.
Mailing address: 410056, Russia, Saratov, ul. Volskaya, d. 1.
- VINNITSKIY
Danil
Vladimirovich** Doctor of Law, Professor, Head of the Department of Financial Law of the Ural State Law University, Director of the BRICS Law Institute.
Mailing address: 620137, Russia, Ekaterinburg, ul. Komsomolskaya, d. 21.
- VOSKOBITOVA
Lidia
Alekseevna** Doctor of Law, Professor, the Head of the Department of Criminal Procedure Law of the Kutafin Moscow State Law University, Honored Worker of the Higher Professional Education of the Russian Federation.
Mailing address: 125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9.
- ZAKHAROV
Vladimir
Viktorovich** Doctor of Law, Professor, Chairman of Arbitration Court of Kursk Region.
Mailing address: 305000, Russia, Kursk, ul. Radischeva, d. 33.
- ZANKOVSKIY
Sergey
Sergeevich** Doctor of Law, Professor, Acting Head of the Business and Corporate Law Sector, Chief Scientific Officer of the Institute of State and Law of the Russian Academy of Sciences.
Mailing address: 119019, Russia, Moscow, ul. Znamenka, d. 10
- Editorial Board**
- KASHANINA
Tatyana
Vasilyevna** Doctor of Law, Professor of the Department of Theory of the State and Law of the Kutafin Moscow State Law University, Professor.
- KLEPITSKIY
Ivan
Anatolyevich** Doctor of Law, Professor of the Department of Criminal Law of the Kutafin Moscow State Law University, Professor.
- MIKHAILOV
Sergey
Mikhailovich** Acting Head of the Department of Civil and Administrative Court Proceedings of the Kutafin Moscow State Law University, PhD in Law, Associate Professor.
- OSAVELYUK
Aleksey
Mikhailovich** Doctor of Law, Professor of the Department of Constitutional and Municipal Law of the Kutafin Moscow State Law University.
- PODUZOVA
Ekaterina
Borisovna** PhD in Law, Associate Professor of the Department of Civil Law of the Kutafin Moscow State Law University.
- SOKOLOVA
Natalya
Aleksandrovna** Doctor of Law, Head of the Department of International Law of the Kutafin Moscow State Law University, Associate Professor.
-

СОДЕРЖАНИЕ

ТЕОРИЯ ПРАВА

- Корнев А. В. *Дигитализация права: проблемы и перспективы* 11

ФИЛОСОФИЯ И ЭТИКА ПРАВА

- Артемов В. М. *Нравственно-философский анализ практики цифровизации в современном образовании для юристов: взгляд в будущее* 19

ФИНАНСОВОЕ ПРАВО

- Ситник А. А. *Финансовые технологии: понятие и виды* 27

БАНКОВСКАЯ СИСТЕМА И БАНКОВСКАЯ ДЕЯТЕЛЬНОСТЬ

- Камалян В. М. *Правовые риски использования цифровых технологий в банковской деятельности* 32

ГРАЖДАНСКОЕ И СЕМЕЙНОЕ ПРАВО

- Аюшеева И. З. *Особенности гражданско-правового регулирования отношений по предоставлению в пользование недвижимого имущества в условиях развития экономики совместного потребления (sharing economy)* 40

- Гринь О. С. *Трансформации требований к форме договоров с учетом развития цифровых технологий* 49

ГРАЖДАНСКОЕ И АДМИНИСТРАТИВНОЕ СУДОПРОИЗВОДСТВО

- Черных И. И. *Правовое прогнозирование в сфере гражданского судопроизводства в условиях развития информационных технологий* 58

ПРЕДПРИНИМАТЕЛЬСКОЕ И КОРПОРАТИВНОЕ ПРАВО

- Ершова И. В., Трофимова Е. В. *Майнинг и предпринимательская деятельность: в поисках соотношения* 73

- Егорова М. А. *Биткоин как особый вид криптовалюты: понятие, значение и перспективы правового регулирования в предпринимательской деятельности* 83

ПРАВОВАЯ ОХРАНА РЕЗУЛЬТАТОВ ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

- Гринь Е. С., Королева А. Г. *Формирование базовых моделей охраны технологий виртуальной и дополненной реальности в сфере права интеллектуальной собственности* 90

ТРУДОВЫЕ ОТНОШЕНИЯ И СОЦИАЛЬНОЕ ОБЕСПЕЧЕНИЕ

- Лютов Н. Л. *Адаптация трудового права к развитию цифровых технологий: вызовы и перспективы* 98

УГОЛОВНОЕ ПРАВО

- Арямов А. А., Грачева Ю. В. *Цифровизация: уголовно-правовые риски в сфере экономики* 108



Чучаев А. И., Маликов С. В. *Ответственность за причинение ущерба высокоавтоматизированным транспортным средством: состояние и перспективы* 117

УГОЛОВНЫЙ ПРОЦЕСС

Антонович Е. К. *Использование цифровых технологий при допросе свидетелей на досудебных стадиях уголовного судопроизводства (сравнительно-правовой анализ законодательства Российской Федерации и законодательства некоторых иностранных государств)* 125

Масленникова Л. Н. *Трансформация досудебного производства в начальный этап уголовного судопроизводства, обеспечивающий доступ к правосудию в эру Industry 4.0* 137

Обидин К. В. *О соотношении основания для возбуждения уголовного дела и оснований для предъявления обвинения в условиях цифровизации уголовного судопроизводства* 147

АДВОКАТУРА И НОТАРИАТ

Гаврилов С. Н., Володина С. И. *Информационная (цифровая) экосистема адвокатуры в контексте экосистемы цифровой экономики России* 156

КРИМИНАЛИСТИКА И КРИМИНОЛОГИЯ. СУДЕБНАЯ ЭКСПЕРТИЗА

Антонян Е. А., Аминов И. И. *Блокчейн-технологии в противодействии кибертерроризму* 167

Семикаленова А. И., Рядовский И. А. *Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики* 178

ИНТЕГРАЦИОННОЕ ПРАВО

Барабашев А. Г., Пономарева Д. В. *Защита персональных данных и научно-исследовательская деятельность: опыт правового регулирования ЕС* 186

СУДЕБНАЯ СИСТЕМА И СУДОУСТРОЙСТВО

Лаптев В. А., Соловяненко Н. И. *«Судебное облако»: правовые вопросы структурирования и защиты данных* 195

CONTENTS

THEORY OF LAW

- Kornev A. V. *Digitalization of Law: Challenges and Prospects* 11

PHILOSOPHY AND ETHICS OF LAW

- Artemov V. M. *Moral and Philosophical Analysis of Digitalization
in Modern Education for Lawyers: A Look into the Future* 19

FINANCIAL LAW

- Sitnik A. A. *Financial Technologies: The Concept and Types* 27

BANKING SYSTEM AND BANKING ACTIVITIES

- Kamalyan V. M. *Legal Risks of Using Digital Technologies in Banking* 32

CIVIL AND FAMILY LAW

- Ayusheeva I. Z. *Peculiarities of Civil Law Regulation of Relations Concerning
Granting Real Estate for Use in the Context of Development
of Shared Consumption Economy (Sharing Economy)* 40

- Grin O. S. *Transformation of Contract Form Requirements
Based on the Development of Digital Technologies* 49

CIVIL AND ADMINISTRATIVE PROCEEDINGS

- Chernykh I. I. *Legal Forecasting in the Field of Civil Proceedings
in the Context of Development of Information Technologies* 58

BUSINESS AND CORPORATE LAW

- Ershova I. V., Trofimova E. V. *Mining and Business Activities: in Search of the Balance* 73

- Egorova M. A. *Bitcoin as a Special Kind of Cryptocurrency:
A Concept, Meaning and Prospects of Legal Regulation in Business* 83

LEGAL PROTECTION OF RESULTS OF INTELLECTUAL ACTIVITY

- Grin E. S., Koroleva A. G. *Formation of Basic Models of Protection
of Technologies of Virtual and Augmented Reality
in the Context of Intellectual Property Rights* 90

LABOUR RELATIONS AND SOCIAL SECURITY

- Lyutov N. L. *Labour Law Adaptation to the Digital
Technologies: Challenges and Perspectives* 98

CRIMINAL LAW

- Aryamov A. A., Gracheva Yu. V. *Digitalization: Criminal Law Risks in the Economy* 108

- Chuchaev A. I., Malikov S. V. *Responsibility for Causing Harm
by a Highly Automated Vehicle: State and Perspectives* 117



CRIMINAL PROCEDURE

- Antonovich E. K.** *The Use of Digital Technologies in the Interrogation of Witnesses in the Pre-trial Stages of Criminal Proceedings (Comparative Legal Analysis of the Russian Federation Legislation and the Legislation of Some Foreign Countries)* 125
- Maslennikova L. N.** *Transformation of Pre-trial Proceedings in the Initial Stage of Criminal Proceedings, Ensuring Access to Justice in the Industry 4.0 Era* 137
- Obidin K. V.** *The Ratio of the Grounds for Initiating a Criminal Case and the Grounds for Charges in Conditions of Digitization of Criminal Proceedings* 147

ADVOCACY AND NOTARY

- Gavrilov S. N., Volodina S. I.** *IT (digital) Ecosystem of the Advocacy in the Context of Russian Digital Economy Ecosystem* 156

CRIMINALISTICS AND CRIMINOLOGY FORENSIC EXAMINATION

- Antonyan E. A., Aminov I. I.** *Blockchain Technology in Countering Cyber Terrorism* 167
- Semikalenova A. I., Ryadovskiy I. A.** *The Use of Special Knowledge in Detecting and Fixing Digital Traces: Analysis of Modern Practice* 178

INTEGRATION LAW

- Barabashev A. G., Ponomareva D. V.** *Personal Data Protection and Research Activities: EU Legal Regulation Experience* 186

JUDICATURE AND COURT SYSTEM

- Laptev V. A., Solovyanenko N. I.**
«Judicial Cloud»: Legal Issues of Data Structuring and Protection 195

Дигитализация права: проблемы и перспективы¹

Аннотация. В статье рассматриваются отдельные проблемы, которые связаны с цифровизацией правовой среды и некоторых видов юридической деятельности. К их числу относится возрастание электронного документооборота, так называемое «электронное правосудие», электронно-коммуникативные технологии в законотворческой и правоприменительной деятельности. Обосновывается тезис о неизбежности трансформации правовой системы под воздействием информационно-коммуникативных технологий. Показывается опыт некоторых зарубежных стран, в которых технологии четвертой промышленной революции применяются достаточно давно. Очерчиваются проблемы, которые возникают с применением цифровых технологий в юридической сфере. Отмечается роль цифровой информации и ее значение для принятия управленческих решений. Отражаются изменения, связанные с правовыми формами деятельности государства. Делаются прогнозы относительно развития системы права и системы законодательства, профессии юриста и некоторых видов юридической деятельности в ближайшей временной перспективе. Обосновывается тезис о том, что развитие технологий является едва ли не главным фактором конкурентоспособности современного государства.

Ключевые слова: право, государство, правовая система, система права, система законодательства, технологии, цифровизация, юриспруденция.

DOI: 10.17803/1994-1471.2019.103.6.011-018

С 2000-х гг. мир переходит к VI технологическому укладу, или к четвертой промышленной революции. Разумеется, этот процесс не везде идет одинаково. Мы вступаем в так называемую цифровую эпоху, которая может изменить и уже серьезно меняет наш мир. В некоторых сферах несколько впереди оказались страны Юго-Восточной Азии, и прежде всего Китай. Серьезные прорывы в этом направлении имеются и в США, странах ЕС. Например, на сегодняшний день Китай обгоняет США по объему электронных платежей в 50 раз. В течение

полтора-двух лет Поднебесная планирует отказаться от денег в их привычном выражении. Это, конечно же, не говорит о том, что самая передовая держава затормозила свое развитие. Просто цифровые технологии шире входят в быт тех стран, которые когда-то относили к третьему миру. Но эти государства сейчас так серьезно продвинулись, что прежние характеристики уже не соответствуют действительности. Есть и еще один фактор, который создает впечатление опережающего развития «азиатских тигров». Прежде всего динамика изменений, которые

¹ Статья подготовлена при поддержке РФФИ, проект № 18-29-16114.

© Корнев А. В., 2019

* Корнев Аркадий Владимирович, доктор юридических наук, профессор, заведующий кафедрой теории государства и права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)

Lab.ktgp@msal.ru

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

поражают воображение. В этом географическом регионе наблюдается взрыв пассионарности (в терминологии Л. Н. Гумилева). Многие страны веками пребывали в состоянии экономической спячки. Но все изменилось во второй половине XX в. В некоторых странах Юго-Восточной Азии к руководству пришли люди, которые стали внедрять западные модели организации экономической деятельности и делать ставку на развитие технологий. Не стоит забывать, что первой страной, которая перешла на западную модель экономики, была Япония. Она стала проводить масштабные изменения еще в первой трети XIX в. Поражение в Русско-японской войне 1905 г. можно объяснить тем, что правящие круги Российской империи воспринимали Японию, руководствуясь прежними стереотипами о ней как о замкнутой, отсталой, аграрной стране. К слову сказать, историческое развитие Японии давало к этому определенные поводы. Военные правители Японии — сёгуны из династии Токугава — практически на 300 лет закрыли страну от внешнего мира. Ни один японец фактически не мог покинуть страну, и ни один иностранец не имел легальной возможности посетить ее. Конечно, это не способствовало развитию страны, и положение дел со временем было исправлено. Не стоит забывать, что еще каких-то 40—50 лет тому назад Япония по уровню технологического развития была впереди планеты всей. Однако США все сделали для того, чтобы несколько придержать Японию. И надо сказать, что им это удалось.

Сейчас в научной литературе встречается много терминов, словосочетаний, конструкций, которые пока не имеют общепринятого значения. К таким категориям, безусловно, относят цифровую экономику, которая, как считают некоторые исследователи, является продолжением информационной экономики. Такой подход имеет как своих сторонников, так и оппонентов. Последние не без некоторых оснований в этих категориях видят определенное преувеличение. Они отмечают некоторую искусственность

вышеназванных конструкций. Информация, как и цифра, не меняет природу экономических отношений. Изменения касаются, по их мнению, лишь формы.

Надо сказать, что такая логика не лишена оснований. Информация, пусть и в цифровой форме, принципиально не трансформирует характер создания новых ценностей. Она лишь вносит определенные технологические новшества в сам характер производства и обмена товарами, более широко — благами. Однако стоит согласиться с тем, что информационная экономика является коммуникационной структурой и технической основой для последующей цифровой трансформации.

Высказывается мнение, что «...цифровую экономику, вырастающую на базе информационной экономики, можно определить как ее продолжение в новом качестве после беспрецедентного технологического прорыва в результате четвертой промышленной революции².

В процессе четвертой промышленной революции производство развивается за счет познавательной деятельности человека. «... Четвертая промышленная революция связана не только с умными и взаимосвязанными машинами и системами, ее спектр действия значительно шире. Одновременно возникают волны дальнейших прорывов в самых различных областях: от расшифровки информации, записанной в человеческих генах до нанотехнологий, от возобновляемых энергоресурсов до квантовых вычислений. Именно синтез этих технологий и их взаимодействие в физических, цифровых и биологических доменах составляют фундаментальное отличие четвертой промышленной революции от всех предыдущих революций³.

В современных условиях практически любые решения принимаются на основе цифровой информации — вот главный конек информационной и цифровой экономики. В своей основе она усиливает эффекты от работы с ценовой информацией и открывает новые возможности, снижает рыночные барьеры и предлагает новые

² Сафрончук М. В. Цифровая поступь революции (четвертая промышленная революция и цифровая трансформация) // Экономика и управление: проблемы, решения. 2017. № 11. Т. 5. С. 52.

³ Шваб К. Четвертая промышленная революция. М., 2019. С. 16—17.

принципы координации. В ближайшее десятилетие на формирование цифровой экономики в мире будет оказывать влияние использование технологий больших данных, искусственного интеллекта, интернета вещей и для вещей, распределенного хранения и обработки данных, а также облачных, аддитивных, в организации бизнеса — платформенных⁴.

На наших глазах может сформироваться и уже формируется совершенно новая социальная реальность. Перед наукой могут возникнуть проблемы, на которые она, казалось бы, давно дала ответы. Например, расшифровка генома человека, а также соединение биологического с технологическим вновь может поставить проблему человека, причем не только в философском, социологическом, но и в правовом аспекте. Актуализируются вопросы совершенно другого понимания таких категорий, как субъект права, правоспособность, дееспособность и пр. За счет вживления чипов в ткань можно управлять здоровьем человека, избавлять его от многих заболеваний, включая наследственные. Однако возникает опасность внешнего управления самим человеком. Все это может поставить множество проблем перед «классической юриспруденцией».

Констатируется следующий тезис: «Фактически наука развивается такими темпами, что на пути прогресса встают уже не технические, а юридические, нормативные и этические ограничения. Самые сложные проблемы, связанные с разработкой социальных норм и соответствующих нормативных актов, возникают именно в сфере биологии. Перед нами встают новые вопросы, связанные с тем, какое значение это имеет для человека, какие данные о нашем теле и состоянии здоровья могут или должны быть опубликованы и какие права и обязанности возникают у нас с вами в связи с изменением генетического кода будущих поколений»⁵.

В связи с этим ряд основополагающих статей Конституции Российской Федерации несколько утрачивают смысл, назначение, если угодно охранительный характер. Например, ст. 2 — «Че-

ловек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина — обязанность государства». Возникают вопросы и с реализацией положений ст. 21, которая гласит: «Достоинство личности охраняется государством. Ничто не может быть основанием для его умаления». В современных условиях проблематичной становится и ст. 23 Конституции РФ: «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения». Статья 24 утверждает положение о том, что «сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускается».

Очевидно, что в условиях электронно-информационной среды некоторые права и свободы защитить будет очень сложно. Здесь могут конкурировать интересы личности, общества и государства. К примеру, личные сведения о гражданине хранятся в базах данных различных структур, получить доступ к которым продвинутым пользователям не составляет никакого труда. По факту это создание благоприятных условий для всех видов мошенничества уже сегодня, а что же будет завтра, если сведения о гражданине и человеке будут содержать данные, которые они по разным причинам не хотели бы предавать огласке. Например, перспектива создания электронных паспортов, которые фактически будут содержать всю информацию о человеке. Конфиденциальность сведений не может быть гарантирована, а значит, ими может фактически пользоваться любой желающий в самых разных целях, не исключая, естественно, криминальные. В силу этого в настоящее время очень остро стоит проблема обеспечения сохранности баз данных. К примеру, крупнейшие банки мира регулярно подвергаются хакерским атакам, и даже они не могут гарантировать абсолют-

⁴ Основы цифровой экономики / под ред. М. И. Столбова, Е. А. Бренделевой. М., 2018. С. 31.

⁵ Шваб К. Указ. соч. С. 35—36.

ную безопасность сведений о своих клиентах и об их вкладах.

В перспективе многие привычные нам институты могут измениться до такой степени, что потребуют совершенно другой интерпретации, включая правовые аспекты. Статья 38 Конституции РФ закрепляет: «Материнство и детство, семья находятся под защитой государства». Любопытно, что материнство находится под защитой государства, а отцовство почему-то нет. Ученые могут к 2025 г. создать искусственную печень. Примерно к этому же времени планируется создать искусственную матку и искусственный сперматозоид. Прогнозируется, что к 2075 г. примерно 70—75 % детей будут создаваться в искусственной среде. Появится возможность создавать так называемых «дизайнерских детей» с предпочтительными физическими и биологическими данными. И как в этих условиях быть с категориями «мать», «отец», «семья», которые помимо святого, поистине сакрального библейского смысла, имеют еще и юридическое значение? Очевидно, что вся система правового регулирования может претерпеть серьезные изменения. Не исключено, что встанет проблема разработки совершенно нового понятийно-категориального аппарата юридической науки и практики.

Основным элементом правовой системы является субъект права. В этой связи может возникнуть ряд проблем. Беспилотные автомобили, самолеты, поезда, роботы-врачи, искусственный интеллект, искусственные люди потребуют коренного пересмотра привычных юридических категорий и создания новых.

По всей видимости, изменится представление об обществе, о характере социальных коммуникаций и т.д. Правовая сфера традиционно предполагает физический контакт субъектов права. Как отмечает Клаус Шваб: «Цифровая революция создает радикально новые подходы, коренным образом изменяющие способ взаимодействия и сотрудничества между отдельными людьми и учреждениями. Например, цепочка блоков, известная как «распределенная база данных», является безопасным протоколом,

в рамках которого сеть компьютеров коллективно заверяет сделку до ее регистрации и подтверждает. Технология, на которой основана цепочка блоков, создает условия для доверия, давая возможность между собой незнакомым людям (которые, таким образом, не имеют оснований доверять друг другу) взаимодействовать, минуя нейтральный центральный орган, то есть банк-кастодиан (банк, осуществляющий хранение ценных бумаг и иных финансовых активов клиентов, а также управляющий этими ценными бумагами. — А. К.) или центральный регистр»⁶.

В настоящее время самым известным применением цепочки блоков является Bitcoin, однако в ближайшее время с развитием новых технологий будет создано много других технологий. Этот процесс будет постоянным. Если сегодня технология цепочки блоков регистрирует финансовые сделки с цифровыми валютами, то в недалеком будущем она будет выполнять роль регистратора самых различных документов юридического характера — от свидетельств о рождении до свидетельств о смерти. Любой вид сделки, которая может быть закодирована, будет регистрироваться таким образом.

Это и есть, по сути, то, что принято в последнее время называть цифровизацией права.

Необходимо отметить, что в эпоху четвертой промышленной революции меняется представление и о государстве. Уже в период третьей промышленной революции (примерно с 1960-х гг.), то есть с развития полупроводников, больших ЭВМ, персональных компьютеров и сети Интернет (начиная с 90-х гг. прошлого столетия) государство, оставаясь организацией политической власти в масштабах всего общества, видоизменяет формы своей деятельности. В последние годы все чаще стало использоваться такое понятие, как «электронное государство». В самом общем виде его образ обозначен в Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы», утвержденной Указом Президента РФ от 9 мая 2017 г. № 203⁷. В литера-

⁶ Шваб К. Указ. соч. С. 32.

⁷ СЗ РФ. 2017. № 20. Ст. 2901.

туре встречаются различные попытки сформулировать понятие электронного государства, которое «...есть политико-правовой феномен, определяющий современный формат взаимодействия государства с обществом на основе использования современных информационных коммуникаций. Электронное государство включает в себя такие элементы, как: электронное правительство, электронное правосудие и электронная демократия»⁸.

Соответственно, электронное правительство представляет собой осуществляемую посредством применения информационно-коммуникационных технологий модель деятельности исполнительных органов государственной власти, муниципальных органов власти и институтов гражданского общества по взаимодействию с населением, нацеленную на повышение уровня оперативности, снижение материальных затрат и удобство получения организациями и гражданами государственных, муниципальных и иных услуг, оказываемых в электронной форме.

Электронная демократия определяется как форма народовластия, при которой воля народа в правотворческом и избирательном процессах выражается при помощи информационных технологий, направленная на поддержку институтов гражданского общества, а также на значительное снижающее влияние административного управленческого фактора в процессе принятия нормативных правовых актов и государственно значимых решений.

Электронное правосудие есть особая форма осуществления государственной деятельности по рассмотрению и разрешению различных категорий дел в электронной форме, включая подачу заявления и прилагаемых к нему документов в электронном виде, ведение судебного процесса с помощью информационных технологий, в том числе вынесение решения по делу, передача его сторонам по электронным сервисам связи и размещение судебной документации на сайтах судов⁹.

Подобная точка зрения, не лишённая оснований, все-таки не может быть безоговорочно принята. Безусловно, информационно-электронные коммуникации меняют формы и методы функционирования традиционных институтов, каковыми являются государство и право. Но это скорее техническая сторона дела. Трудно согласиться с тем, что электронное государство представляет собой «политико-правовой феномен», если использовать эту конструкцию в привычном значении. Феномен означает явление, данное нам в опыте, постигаемом при помощи чувств. Как известно, Кант ввел понятие noumena, который является полной противоположностью феномена, поскольку остается за пределами человеческого опыта и соответственно недоступен человеческому созерцанию.

Если взаимодействие власти с населением приобретает формат информационных коммуникаций, то неизбежно исчезает эффект «физического контакта» индивида и того, кто принимает решение. В этом случае техническая сторона дела явно доминирует, поэтому именовать современное государство политико-правовым феноменом не совсем правильно. Скорее это симбиоз технологий и власти. Вошедшее в оборот словосочетание «машина власти» в буквальном смысле наполняется другим содержанием и из метафоры превращается в реальность.

Если интерпретацию электронной демократии и электронного правосудия можно принять с известными оговорками, то дефиниция электронного правительства не выдерживает никакой критики. Какое же это правительство, если в качестве субъектов взаимодействия в формате информационно-коммуникативных технологий с одной стороны представлены исполнительные органы власти, муниципальные органы власти и институты гражданского общества (!), а с другой — население? Не совсем понятно, почему в структуру правительства необходимо включать органы местного самоуправления, и уж тем более институты гражданского общества.

⁸ Киселев А. С. Формирование идеи электронного государства и особенности ее реализации: теоретико-правовое исследование : автореф. дис. ... канд. юрид. наук. Белгород, 2018. С. 9.

⁹ Киселев А. С. Указ. соч. С. 10.

Все эти подходы так или иначе отражают некоторую искусственность многих конструкций, которые стали активно обсуждаться в публичном пространстве, в том числе и в юридической науке и практике. Информационно-электронная среда активно завоевывает пространство, включая правовое. К примеру, ряд законопроектов, разработанных в Государственной Думе, уже составлен на языке программирования. Использование технических возможностей значительно облегчает подготовку законопроектов, позволяет делать их максимально лаконичными, согласованными, непротиворечивыми и беспробельными. Проявление всех этих недостатков все равно будет связано с так называемым человеческим фактором. До появления искусственного интеллекта в полном смысле этого слова еще минимум 50—60 лет. До этого времени в отношениях человек-машина будет господствовать человек. Да и в дальнейшем он вряд ли откажется от своей власти над действительностью, какую бы форму она ни принимала.

Современное российское понимание так называемого электронного правосудия, как показывает анализ литературы, свидетельствует о том, что в нем делается акцент на технической стороне дела. То есть обычно пишут об электронной форме подачи заявлений, фиксации материалов судебных заседаний, оповещении участников дела, размещении решений судов на соответствующих сайтах и т.д. Между тем во многих странах уже пошли дальше. В Англии, например, разработаны программы, которые позволяют решать многие категории дел по существу. Иными словами, в машину закладывается фабула дела и на основе массива статутного и прецедентного права она выдает решение. Автоматизация правосудия набирает обороты. Сеть позволяет осуществлять контакты без физического взаимодействия. В этом процессе есть как свои минусы, так и свои плюсы.

Например, многие правоустанавливающие документы сегодня хранятся в электронной форме. Чтобы получить его в «бумажном» варианте, необходимо заплатить определенную сумму.

Граждане, как правило, предпочитают иметь документы в традиционной форме. Во-первых, в силу инерции. Во-вторых, бумажный вариант представляется более надежным носителем. Информационно-электронная среда подвергается и будет подвергаться значительным рискам, вплоть до полного уничтожения информации. Общество с некоторым опасением относится к нововведениям. Это одна сторона вопроса. Вторая же заключается в том, что по уровню доступа к Интернету Российская Федерация явно не в числе лидеров. Особенно эта проблема касается сельского населения. Да и потом, уровень «цифровой» грамотности все еще оставляет желать лучшего.

Юридическая сфера, как и другие, в скором времени будет подвергаться еще большей автоматизации. Темпы будут только нарастать. Экспертное сообщество прогнозирует, что в ближайшие 15—20 лет 47—50 % профессий будут полностью автоматизированы. В перспективе может серьезно измениться сам характер юридической деятельности, профессия юриста в целом. Единства мнений тут нет. Одни говорят о постепенном отмирании юриспруденции как профессии, другие придерживаются противоположной точки зрения. К числу вторых относится Энтони Аткинсон, известный ученый-экономист, специалист в области распределения доходов в современном мире. По его мнению, рабочие места с высоким риском автоматизации находятся преимущественно в офисном, управленческом и торговых секторах, а также в сфере услуг. К группе низкого риска относятся рабочие места в сферах здравоохранения, образования, науки, юриспруденции, искусства, муниципальных услуг и средств массовой информации. Это естественно, считает он, ибо в этих профессиях важны такие человеческие качества, как общительность, отзывчивость, нестандартность мышления, а также умение убеждать и договариваться¹⁰.

Правда, так думают далеко не все. Например, Крис Скиннер не без удовольствия утверждает: «Сочетание распределенных ре-

¹⁰ Аткинсон Э. Неравенство. Как с ним быть? М., 2018. С. 177.

¹¹ Скиннер К. Цифровой человек. М., 2019. С. 112.

естров и искусственного интеллекта приведет к пересмотру правовой сферы и к ее дигитализации — юристы станут не нужны. Прекрасно, правда?»¹¹

Профессии традиционно делят на физические (мануальные) и когнитивные. В первом случае доминирует физический труд и делается акцент на трудовые навыки. В когнитивных профессиях преобладают элементы творчества, нестандартность мышления, креативность.

Но даже нетворческое содержание профессии юриста оставляет ее востребованной в будущем. Никакие компьютеры, включая квантовые, не в состоянии понимать содержание таких категорий, как гуманизм, справедливость, добрая совесть, этика, мораль, нравственность, свобода, ответственность. Без всего этого правовое регулирование невозможно. Если, конечно, человечество не откажется от тех институтов, которые придают смысл всякой человеческой деятельности и лежат в основе нашей жизни.

Право — явление цивилизации и культуры, один из фундаментов общества. Оно обречено следовать за теми процессами, которые будут происходить сегодня и завтра. В принципе, право в настоящее время не только у нас, но и в технологически развитых странах пока отстает от темпов четвертой технологической революции. Эта проблема, которая стоит на повестке дня и ждет своего решения. Не надо бесконечно повторять тезис об отставании правового регулирования от технологических преобразований. Иногда их нужно тормозить, например в биотехнологиях. Не все, конечно. Но это тема отдельного разговора.

Таким образом, современные технологии неуклонно преобразуют действительность. Соединение физического, биологического и цифрового миров создает новую реальность, в которой праву предстоит играть ту же привычную роль, но уже в других, преимущественно цифровых формах.

БИБЛИОГРАФИЯ

1. *Аткинсон Э.* Неравенство. Как с ним быть? — М., 2018. — 536 с.
2. *Киселев А. С.* Формирование идеи электронного государства и особенности ее реализации: теоретико-правовое исследование : автореф. дис. ... канд. юрид. наук. — Белгород, 2018. — 22 с.
3. *Сафрончук М. В.* Цифровая поступь революции (четвертая промышленная революция и цифровая трансформация) // Экономика и управление: проблемы, решения. — 2017. — № 11. — Т. 5 (71). — С. 52—56.
4. *Скиннер К.* Цифровой человек. — М., 2019. — 304 с.
5. *Столбова М. И., Бренделева Е. А.* Основы цифровой экономики. — М., 2018. — 238 с.
6. *Шваб К.* Технологии четвертой промышленной революции. — М., 2018. — 320 с.
7. *Шваб К.* Четвертая промышленная революция. — М., 2019. — 209 с.

Материал поступил в редакцию 6 мая 2019 г.

DIGITALIZATION OF LAW: CHALLENGES AND PROSPECTS¹²

KORNEV Arkadiy Vladimirovich, Doctor of Law, Professor, Head of the Department of Theory of the State and Law of the Kutafin Moscow State Law University (MSAL)
Lab.ktgp@msal.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

Abstract. *The article deals with the problems associated with digitalization of the legal environment and some types of legal activities. The problems under consideration include the increase in electronic document flow, the so-called «electronic justice», electronic communication technologies in legislative and law enforcement activities. The author substantiates the premise concerning the inevitability of transformation of the legal system under the influence of information and communication technologies. The article describes the experience of some foreign countries where the technologies of the Fourth Industrial Revolution have been used for quite a long time. The problems that arise due to the use of digital technologies in the legal sphere are outlined. The author highlights the role of digital information and its importance for managerial and administrative decision-making and maps changes associated with legal forms of the activity of the State. Predictions are made regarding the development of the legal system and the system of legislation, legal profession and some types of legal activities in the short term. The author substantiates the premise that the development of technologies is almost the main factor of competitiveness of a modern State.*

Keywords: *law, State, legal system, system of law, system of legislation, technology, digitalization, jurisprudence.*

REFERENCES (TRANSLITERATION)

1. Atkinson E. Neravenstvo. Kak s nim byt'? — M., 2018. — 536 s.
2. Kiselev A. S. Formirovanie idei elektronogo gosudarstva i osobennosti ee realizacii: teoretiko-pravovoe issledovanie : avtoref. dis. ... kand. jurid. nauk. — Belgorod, 2018. — 22 s.
3. Safronchuk M. V. Cifrovaya postup' revolyucii (chetvertaya promyshlennaya revolyuciya i cifrovaya transformaciya) // Ekonomika i upravlenie: problemy, resheniya. — 2017. — № 11. — Т. 5 (71). — С. 52—56.
4. Skinner K. Cifrovoj chelovek. — M., 2019. — 304 s.
5. Stolbova M. I., Brendeleva E. A. Osnovy cifrovoj ekonomiki. — M., 2018. — 238 s.
6. Shvab K. Tekhnologii chetvertoj promyshlennoj revolyucii. — M., 2018. — 320 s.
7. Shvab K. Chetvertaya promyshlennaya revolyuciya. — M., 2019. — 209 s.

¹² The article was prepared with the support of RFBR, project No. 18-29-16114.

ФИЛОСОФИЯ И ЭТИКА ПРАВА

В. М. Артемов*

Нравственно-философский анализ практики цифровизации в современном образовании для юристов: взгляд в будущее¹

Аннотация. В статье с нравственно-философских позиций анализируется феномен цифровизации в современном образовании на примере юридического вуза и в аспекте осмысления возможного будущего (наследуемое из прошлого должно быть человеческим, разумным и жизнеспособным). На основе анализа практики цифровизации и ее последствий, включая образовательное поле юридического университета, позиционируется подход, согласно которому преподаватели призваны не просто давать молодежи определенную сумму знаний, но и выстраивать морально оправданную, перспективную парадигму их должного применения в плане развития и совершенствования человека и общества, включая отдельные его институты, в том числе связанные с предпринимательской деятельностью.

Ключевые слова: образование для юристов, цифровизация, морально оправданная парадигма должного применения знаний, человек, общество, предпринимательская деятельность.

DOI: 10.17803/1994-1471.2019.103.6.019-026

Перед тем как приступить к рассмотрению вопросов, входящих в предмет исследования данной статьи, хотелось бы внести ясность относительно темы настоящей работы в связи с коллективным исследованием феномена цифровизации применительно к юридическому бизнес-образованию. *Философия и ее вершинная часть — этика — по определению призваны подниматься на достаточно высо-*

кий уровень абстрагирования и идеализации. Такое призвание не отодвигает нас дальше от самой действительности, а, наоборот, приближает к ней, но, правда, в контексте максимального масштаба, в сущностном аспекте и с учетом высокого социокультурного идеала.

В указанном смысле нами вводится и *фактор будущего.* Этика как *практическая философия по своей природе в целом оптимистична*

¹ Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16081 «Трансформация концептуальных основ подготовки юристов для сферы бизнеса в условиях цифровой экономики».

© Артемов В. М., 2019

* Артемов Вячеслав Михайлович, доктор философских наук, профессор кафедры философии и социологии Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), научный руководитель клуба «Нравственное измерение права»
vyach_artemov@mail.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

и всегда ориентирует на некий личностный и социальный идеал. В этом ключе вполне оправданно исходить из обоснованного предположения, условно говоря, светлого будущего. Всегда хочется верить, что последнее, наследуя лучшее из прошлого, будет достаточно *человечным, разумным и жизнеспособным*.

Речь идет не просто о некоем благом пожелании или безосновной мечте. В известном смысле такая чувственно-эмоциональная и мысленная установка не только составляет неотъемлемую часть уверенности в завтрашнем дне, но и является некоей *внутренней опорой применительно к настоящему*. Думаю, *наша уверенность в себе и других, что называется, здесь и сейчас предполагает вполне определенный образ того, что будет, точнее — должно быть*. В связи с этим вспоминается знаменитое кантовское «должен — значит, можешь». Данное классическое положение, на наш взгляд, следует рассматривать в качестве своеобразного стержня *методологии социального конструирования, особенно образования*.

Так, хочется верить, что на личностном уровне в обозримом будущем *свобода* не только останется, но и в значительной степени усилит свою связь с *нравственностью*, прежде всего *ответственностью как социальным проявлением добра; разум как высшее измерение сознания не растворится в голом расчете* и не опустится до уровня примитивного обывательского здравого смысла, достаточного лишь применительно к «четырем стенам домашнего обихода»; не уступит первенство искусственному интеллекту и в целом цифре, *возвышаясь над обыденностью, проникая в сущность, схватывая и разрешая имеющиеся противоречия*; в качестве скреп общества будут выступать *общие приоритетные ценности (нравственность, свобода, социальная справедливость, истина, правда и т.п.)*, глубокое понимание и последовательная реализация которых обеспечат устойчивое существование и совершенствование *социокультурного целого, включая его собственно правовую часть*.

Возвращаясь к *образу будущего как опоре настоящего*, хочется подчеркнуть, что наличие цели и идеала делает нас людьми в собственном смысле слова, субъектами культуры. Последняя не может жить только сегодняшним днем: она как стрела летит из прошлого через настоящее в будущее; и если остановится, то перестанет быть тем, чем она призвана быть. Поэтому *даже прошлое ждет от нас своеобразной «поддержки», подтверждения того, что оно не прошло бесследно и имеет вполне определенный смысл*. В этой связи вспоминается мысль Виктора Мари Гюго о том, что наша жизнь — путешествие, идея — путеводитель. Нет путеводителя — и все останавливается. Цель утрачена, и сил как не бывало.

Что касается нынешнего этапа развития нашей страны, то утверждена программа «Цифровая экономика», целью которой выступает организация системного развития и *внедрения цифровых технологий во все области жизни*. Тут-то как раз и видится опасность не столь редкого для отечественной и не только истории *перехлеста*. Экономическая необходимость, трактуемая слишком упрощенно и неоправданно широко, может привести к еще бóльшим проблемам. Из очередного сугубо экономического проекта она *может превратиться в монстра, пожирающего все вокруг*. Главной мишенью, увы, может стать сам человек.

Фактически источники *цифровизации*, о чем откровенно пишут западные авторы, — чисто экономические. Вот что мы, к примеру, читаем в одном из новейших трудов: «Как заметили Питер Деннинг (Peter Denning) и Тед Льюис (Ted Lewis), из закона Рока следует, что размер рынка для каждого нового поколения кристаллов должен быть как минимум в два раза больше существующего рынка — только так можно экономически оправдать расходы на новые производственные мощности»². Где здесь человек, общество, тем более справедливое? *Получается, что наше сущностное, человеческое заменяется узко потребительскими интересами. Отсюда явный интерес скорее к психологии, чем к философии, особенно применительно*

² Шваб К. Технологии четвертой промышленной революции. М. : Эксмо, 2018. С. 95.

к маркетингу. «Частые повторения — надежный способ заставить людей поверить неправде, — пишет лауреат Нобелевской премии Даниэль Канеман, — потому что различить истину и ощущение чего-то знакомого нелегко»³. Применение подобных приемов значительно упрощается, когда кем-то включаются *новейшие технологии*. Таким образом, последние ни хороши, ни плохи сами по себе: *все зависит от того, кто и с какой целью их применяет*.

Подобная ситуация особенно опасна применительно к *науке и образованию*. Тут, на наш взгляд, особенно остро проявляют себя по крайней мере *три тенденции*. Первая из них во многом внутренняя и связана с *неоправданными ожиданиями, даже чрезмерными и совсем не безобидными фантазиями относительно каких-то прорывных достижений в сфере создания неких, условно говоря, машин и технологий, которые будто бы способны не только достичь уровня человеческого интеллекта и даже чувств, но и превзойти их*. Остается вопрос: «Зачем готовить себе тех, кто выбросит всех нас на свалку истории, да еще и радоваться этому обстоятельству?» В этой связи вспоминаются филигранно точные нравственно-философские аргументы известного мыслителя советской эпохи Э. В. Ильенкова против подобных фантазий внутри самой научной элиты. Приводя позицию одного тогдашнего академика о возможности создания «Сверхчеловека», философ подчеркивает, что последняя ведет к исключению из поля зрения современности «самого человека», то есть «высшего и самого интересного предмета для человека»⁴.

Вторая тенденция вытекает из первой. Речь идет о своеобразном «*головокружении от успехов*» на *технично-технологическом поле*, когда только что появившееся новое безапелляционно пытается вытеснить имеющееся, проверенное временем, действительно надежное. *Здесь что-то похоже на моду, но гораздо опаснее*.

Один критически настроенный западный философ заметил, что вещи оседлали человека и гонят его вскачь. Перефразируя, можно вещи заменить деньгами, в том числе виртуальными и т.п. *Опять же встает вопрос: «Куда гонят и почему человек на все соглашается?»* В этой связи нельзя не назвать одну из характерных примет современной цивилизации — ускорение. Привычное «хочешь жить — умей вертеться» дополняется «выживанием скорейшего». Социология, в частности, фиксирует, что в такой ситуации «страдают не только те, кто отстает, но и те, кто успевает. Часто они испытывают сильную усталость, буквально задыхаются от высокого темпа жизни, и им все равно не хватает времени, причем даже на то, что сами они считают для себя главным»⁵.

И наконец, *третья опасная тенденция*, которая подстегивает первую, — *экономическая целесообразность*. Сама по себе она может быть общественно полезной, даже в некоторых случаях спасительной (в сложные периоды социально-исторического развития, например НЭП и т.п.). Сейчас же вырисовывается очень противоречивая ситуация. К примеру, условно говоря, цифровые технологии действительно могут помочь и помогают там, где это уместно. Но, если ситуация доводится до абсурда и допускаются так называемые перехлесты, происходит обратное: *из фактора развития данный феномен превращается в неоправданное препятствие*. Та же разрекламированная акция по якобы бесплатному введению цифрового телевидения, к примеру, в массе случаев выливается в то, что на экране домашнего телевизора остаются только региональные программы. Чтобы вернуть вдруг «исчезнувшие» телеканалы, которые до этого действительно были бесплатны и доступны, нужно идти и приобретать либо приставку, либо новый телевизор. Кому выгодна такая «бесплатность» в условиях официального признания бедности как явления, которого

³ Канеман Д. *Думай медленно... Решай быстро*. М.: АСТ, 2018. С. 85.

⁴ Ильенков Э. В. *Почему мне это не нравится // Об эстетической природе фантазии. Что там в зазеркалье?* М., 2017. С. 112.

⁵ Гофман А. Б. *Festina lente: от культуры ускорения к культуре замедления // Вопросы социальной теории: научный альманах*. 2017. Т. IX. С. 124.

не должно быть? Сомнительно, что обществу. *Представляется, что в любом случае экономика должна находиться под контролем самого общества, а не только отдельных заинтересованных в прибылях корпораций. Тогда и праву будут доверять, а государство будет жизнеспособным и достаточно прочным.*

Полагаем, что представители науки и образования призваны обосновывать и обеспечивать разумность этого контроля. Вообще, образование по природе своей является своеобразным стержнем всей духовной культуры, который выполняет функцию бескорыстной передачи знаний и ценностей от одного поколения к другому. По существу, оно *исключает приоритетную роль какой-либо внешней силы или формы, в том числе цифровой, прежде всего опираясь на личностные усилия и профессиональные качества самих преподавателей.*

Предпринимательская же деятельность предполагает использование разного рода манипуляционных технологий, способных приводить к нужным результатам (в виде прибыли), даже если они не соответствуют или даже противоречат интересам потребителей. Соответственно, исходя из соображений должного положения дел, *образовательное сообщество (особенно в юридическом университете) призвано делать все, чтобы минимизировать действительно вредное в этих технологиях и исключать применение подобных в самом образовательном процессе,* чистота которого является важным фактором совершенствования того же бизнеса.

Думается, что своеобразная подмена образования его видимостью особенно нетерпима применительно к обучающимся в сфере предпринимательской (бизнес-) деятельности. Клас-

сическая философия квалифицирует подобную ситуацию как абсолютизацию формы в ущерб содержанию. Тем более когда речь идет о юридическом обеспечении чистоты этой деятельности. *Думается, органичное соединение возможностей нравственности и права в непростом деле совершенствования последнего — это один из актуальных запросов современного, технологически нагруженного общества. Причем сами новейшие технологии требуют к себе не менее пристального внимания с точки зрения правильного их использования⁶.*

В рассматриваемой сфере деятельности подлинность и глубина знаний о тех же человеке и обществе, об их потребностях, интересах, о закономерностях социокультурного развития, взятых в их должном ценностном русле, — это своего рода спасительный для всего общества научно-образовательный ресурс. Последний имеет вполне определенное нравственно-философское обоснование и соответствующую методологическую направленность. Иначе и проще говоря, *добрые цели могут быть достигнуты только при помощи аналогичных же средств.* К примеру, отсутствие обмана на этапе подготовки будущих субъектов бизнес-деятельности обуславливает минимизацию и искоренению лжи и манипуляций в самой этой деятельности.

Применительно к рассматриваемой теме нужно особо подчеркнуть значимость органичного соединения формы и содержания. Именно содержание, как известно из диалектики, если мы имеем в виду развитие, всегда динамичнее, активнее, чем любая форма. *Важно не стать рабами цифровизации как формы. Она, безусловно, современна и перспективна, но не перестает быть формой и никогда не заменит содержание, тем более самого человека.*

⁶ Определенным шагом в этом направлении стала организованная философско-правовым клубом «Нравственное измерение права» на базе кафедры философии и социологии Университета имени О.Е. Кутафина (МГЮА) Международная научно-практическая конференция «Научно-технологические трансформации в современном обществе: нравственно-философское осмысление и особенности правового регулирования», состоявшаяся 1—2 марта 2019 г. в Университете имени О.Е. Кутафина (МГЮА). Под руководством д. ф. н., проф. кафедры философии и социологии, научного руководителя клуба В. М. Артемова и заведующего кафедрой предпринимательского права, заслуженного юриста РФ, д. ю. н., проф. И. В. Ершовой работала и секция в связи с выполнением исследовательского проекта РФФИ № 18-29-16081 «Цифровое пространство в образовании и науке: требования времени и опасности расчеловечивания».

Многое из того, что было сказано выше, в той или иной степени понимают и сами студенты нашего Университета, то есть будущие юристы. Правда, некоторые просто не замечают многие опасности нагрывшейся цифровизации. Об этом, в частности, свидетельствуют проведенные автором *социологические опросы в молодежной среде и проверки множества студенческих работ*, выполненных чаще всего в форме проблемных эссе на заданную тему. Много говорится о разных гранях цифровизации, о ее возможностях, но корни и негативные последствия зачастую остаются в тени.

Нами были изучены настроения, представления и взгляды студентов по крайней мере четырех курсов и четырех же институтов в связи с проблемой цифровизации в образовании. Так, было проверено несколько десятков (около 90) студенческих творческих работ на тему «Цифровизация в этическом и правовом аспектах: как отличить добро от зла, справедливое от несправедливого?».

В целом можно констатировать, что их авторы не только чувствуют выгоды и опасности применения новейших технологий, но и в основном понимают суть проблемы: под угрозой сами человеческая сущность и будущее человечества. Делается типичный вывод о том, что процесс цифровизации, характерный для современного общества, имеет как положительные, так и отрицательные черты. Важно не переступать тонкую грань, регулировать воздействие последствий цифровизации (особенно на молодое поколение). Очевидно, что мера нарушена и пора активно заниматься исправлением ситуации.

Был также организован и проведен социологически корректный опрос около 100 человек. В частности, выяснилось: при всех тех преувеличениях, которые раздаются со всех сторон относительно, так сказать, «цифрового счастья», только 40 % опрошенных отметили «значительный положительный эффект от ее (цифровизации) применения». 49 % сдержанно утверждают, что из-за последней лишь «несколько повышается качество образования», а 8 % считают, что «практически никакого особого эффекта не было». Но самая важная истина вырисовывается, когда анализируешь ответ на вопрос: «Какие

опасности Вы видите в связи с широким применением цифровизации в университетском образовании?» Думается, здесь как раз и скрывается корень или, иначе сказать, внутренний нерв проблемы применительно именно к интересующей нас сфере деятельности. 59 % отмечают «вытеснение живого общения «преподаватель-студент»»; 45 % обратили внимание на «минимизацию общения в самом учебном коллективе»; 6 %, как это ни странно, указали даже на «уменьшение объемов информации»; 32 % — на «снижение объективности и точности оценивания знаний студента». И только 17 % «не видят особых опасностей».

Но самое важное, на наш взгляд, кроется в ответах на вопрос: «Как быть с этикой, если образование рассматривать в качестве услуги экономического типа?» Затруднившиеся ответить 7 %, очевидно, слабо представляют, что такое этика вообще; 15 % считающих, что «ничего страшного не произойдет, а студентам будет легче жить», практически оказываются на стороне, условно говоря, «плохой» мотивации. Увы, за этим просматривается немногочисленная группа тех, кто либо случайно оказался на образовательном поле элитного вуза, либо просто желает получить «корочку», не прилагая особых усилий в плане освоения сложнейших, прежде всего гуманитарных, дисциплин. Большинство же, что внушает оптимизм, ответили так: *это будет «разрушать сам дух образования как ведущего стержня духовной культуры» (59 %), «снижать нравственность студентов» (19 %)*. Сюда же следует отнести и те 72 %, кто полагают, что «передать нравственные ценности и принципы профессиональной этики юриста через видеолекцию» либо «крайне затруднительно» (21 %), либо *возможно лишь «в ограниченном объеме» (43 %)*, либо вообще «невозможно» (8 %).

В этой достаточно ясной ситуации напрашивается вечный вопрос: «Что делать?» Думаю, что университетские и не только преподаватели должны заниматься тем, чем всегда занимались, но еще более последовательно и содержательно, то есть нести молодежи разумное, доброе и вечное. Никакие цифровые технологии этого не могут заменить. *Абсолютно неприемлемы*

узко направленные экономический и формально-юридический подходы, когда люди выступают в качестве практически неодушевленных предметов, интересующих аналитиков лишь в связи с некими якобы объективными процессами рыночного типа. Игнорирование нравственного измерения человеческой жизни и справедливости как своеобразной меры социально приемлемого ведет к выхолащиванию собственно человеческого в человеке.

Правовая система не должна замыкаться в себе. Опираясь на нравственный фундамент, она призвана двигаться в сторону максимального учета долговременных интересов и ожиданий самих людей, в том числе и применительно к юридическому бизнес-образованию. *Нельзя забывать и о правовом нигилизме, преодоление которого требует от самих юристов истины, справедливости и правды.* Усиливается и значимость прицельного культивирования человеческого в человеке в профессиональной этике, включая ее юридическую составляющую, теоретической и ценностной основой которой исторически и логически выступает именно философия.

Возвращаясь к рассмотренному выше опросу, отметим и откровенные признания студентов в том, что *многие не готовы быть в отрыве от ведущей роли конкретного преподавателя в процессе освоения знаний* и т.п. Кстати, в этой связи нельзя не обратить внимание на то, что вытеснение последнего из учебного процесса является *нарушением принципа свободы образования и в образовании.* Цифровизация может нивелировать некую творческую энергию, рождающуюся в самом образовательном процессе, в том числе во время лекций, когда зритель здесь и сейчас и, что называется, живьем нуждается, условно говоря, в актере, а тот — в зрителе. Проблема нуждается в дальнейшем осмыслении и практических шагах в правильном, то есть спасительном для всех нас, направлении. В этом как раз наша ответственность, которая является оборотной стороной зрелой свободы.

В плане метода, к примеру, определенный интерес представляет позиция Ричарда Вернера: «Метод этики — собеседование с другими, честное и открытое собеседование, которое оставляет *это* за дверями и стремится к наилучшему решению имеющихся проблем... Но, чтобы это работало, необходимо, чтобы кто-то создал сообщество с общими ценностями»⁷. Применительно к рассматриваемой ситуации *следует, на наш взгляд, стремиться к тому, что принято называть взаимопониманием, а еще выше — духовно-нравственным единством.* Именно это в принципе открывает необъятные возможности для личностного самоутверждения, раскрытия человеческой сущности, совершенствования общества, включая и институт права.

Исходя из должного понимания нормального будущего, перед опасностями технократически узко понимаемой цифровизации следует, условно говоря, возвести вполне определенную стену, точнее — систему запретов, с тем чтобы не допустить каких-либо неоправданных действий, корыстных манипуляций, разного рода злоупотреблений или легкомысленных экспериментов, способных разрушать проверенные временем и доказавшие свою состоятельность способы осуществления сложных видов деятельности, особенно в сфере науки и образования. В этой связи представляет интерес известная концепция «негативной этики»⁸, которая может оказаться значимой именно *в позитивно-утверждающем плане, приблизить приемлемое в человеческом отношении будущее.*

Прежде всего, применительно к современным технологиям, включая и цифровизацию, следует позиционировать *запрет на ложь* в самом широком смысле слова. К примеру, специфика современных СМИ, да и средств связи в целом, заключается в том, что с одинаковой скоростью распространяются и правда, и ложь. В современных условиях важно позиционировать личностно-ответственное измерение

⁷ Цит. по: Мораль: разнообразие понятий и смыслов : сборник научных трудов. К 75-летию академика А. А. Гусейнова. М., 2014. С. 437.

⁸ См.: Гусейнов А. А. Нравственность в свете негативной этики // Мораль: разнообразие понятий и смыслов. С. 13—34.

в устных выступлениях и текстах. Думается, что современное отечественное право не должно обслуживать узкокорпоративные интересы, а должно отдавать предпочтение интересам развития и совершенствования всего социо-

культурного целого. Жизнь, человек и его разум — вот «три кита» для общества и права. При этом разум органично включает в себя нравственное измерение, а последнее предполагает принцип абсолютной ценности жизни.

БИБЛИОГРАФИЯ

1. Гофман А. Б. Festina lente: от культуры ускорения к культуре замедления // Вопросы социальной теории : научный альманах. — 2017. — Т. IX. — С. 123—138.
2. Гусейнов А. А. Нравственность в свете негативной этики // Мораль: разнообразие понятий и смыслов : сборник научных трудов. К 75-летию академика А. А. Гусейнова. — М. : Альфа-М., 2014. — С. 13—34.
3. Ильенков Э. В. Почему мне это не нравится // Об эстетической природе фантазии. Что там в зазеркалье? — М. : Либриком, 2017. — С. 94—117.
4. Канеман Д. Думай медленно... Решай быстро. — М. : АСТ, 2018. — 653 с.
5. Шваб К. Технологии четвертой промышленной революции. — М. : Эксмо, 2018. — 320 с.

Материал поступил в редакцию 6 мая 2019 г.

MORAL AND PHILOSOPHICAL ANALYSIS OF DIGITALIZATION IN MODERN EDUCATION FOR LAWYERS: A LOOK INTO THE FUTURE⁹

ARTEMOV Vyacheslav Mikhailovich, Doctor of Philosophy, Professor of the Department of Philosophical and Social Disciplines of the Kutafin Moscow State Law University (MSAL), Academic Director of the Club «Moral Dimension of Law»
vyach_artemov@mail.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

Abstract. *The paper analyzes the phenomenon of digitalization in modern education in the context of moral and philosophical positions on the example of a law university and in light of comprehension of the possible future (what is inherited from the past should be human, reasonable and viable). Based on the analysis of digitalization procedure and its consequences, including in the educational field of a law university, the author introduces an approach according to which teachers are called not only to give young people a certain amount of knowledge, but also to build a morally justified, promising paradigm of proper application of knowledge in terms of development and improvement of the person and society, including their individual institutions that are, inter alia, related to business activities.*

Keywords: *education for lawyers, digitalization, morally justified paradigm of proper use of knowledge, human being, society, entrepreneurial activity.*

⁹ The study was carried out with the financial support of RFBR within the framework of the scientific project No. 18-29-16081 «Transformation of the Conceptual Foundations of Training Lawyers for the Area of Business in the Digital Economy.»

REFERENCES (TRANSLITERATION)

1. *Gofman A. B.* Festina lente: ot kul'tury uskoreniya k kul'ture zamedleniya» // *Voprosy social'noj teorii : nauchnyj al'manah.* — 2017. — T. IX. — S. 123—138.
2. *Gusejnov A. A.* Nравstvennost' v svete negativnoj etiki // *Moral' : raznoobrazie ponyatij i smyslov : sbornik nauchnyh trudov. K 75-letiyu akademika A. A. Gusejnova.* — M. : Al'fa-M., 2014. — S. 13—34.
3. *Il'enkov E. V.* Pochemu mne eto ne nraivitsya // *Ob esteticheskoj prirode fantazii. Chto tam v zazerkal'e?* — M. : Librikom, 2017. — S. 94—117.
4. *Kaneman D.* Dumaj medlenno... Reshaj bystro. — M. : AST, 2018. — 653 s.
5. *Shvab K.* Tekhnologii chetvertoj promyshlennoj revoljucii. — M. : Eksmo, 2018. — 320 s.

Финансовые технологии: понятие и виды

Аннотация. Статья посвящена изучению влияния цифровой экономики на финансовое право. Определено, что в условиях цифровизации экономики новые технологии, с одной стороны, ведут к расширению предмета правового регулирования, а с другой — являются инструментом, способствующим регулированию, администрированию, финансовому контролю и надзору. В работе рассматриваются различные виды финансовых технологий, в первую очередь регулирующие (RegTech) и надзорные (SupTech). По итогам проведенного исследования автор заключает, что термин «регулирующие технологии» в целом является неудачным. Кроме того, следует говорить о том, что в узком понимании финансовые технологии — это совокупность инструментов и методов, применяемых исключительно на финансовых рынках, в широком — используемых во всех областях, связанных с финансовым регулированием, контролем и надзором.

Ключевые слова: финансовые технологии, регулирующие технологии, надзорные технологии, финансовое право, финансы.

DOI: 10.17803/1994-1471.2019.103.6.027-031

Цифровая экономика предполагает широкое внедрение в общественную жизнь новых технологий, имеющее своим главным итогом ускорение обмена информацией, которая становится основным продуктом и движущей силой экономических отношений нового типа.

Процесс цифровизации экономики, основанный на внедрении новых технологий, насчитывает уже несколько десятилетий. Начиная с середины XX в. электронно-вычислительные машины и связанные с ними технологии прошли значительную эволюцию, которая с точки зре-

ния человеческой истории может считаться стремительной. Так, согласно эмпирическому наблюдению одного из учредителей компании Intel Г. Мура, количество транзисторов, размещаемых на кристалле интегральной схемы, удваивается каждые 2 года¹ (закон Мура)². Данный процесс, с одной стороны, ведет к увеличению вычислительных мощностей компьютерной техники, а с другой — к ее миниатюризации. Все это в конечном итоге обуславливает тот факт, что цифровые технологии становятся доступными для широких слоев населения. Именно массовость их использования является движу-

¹ Изначально говорилось об удвоении количества транзисторов в течение одного года, но в 1975 г. данное правило было скорректировано.

² См. подробнее: Антропченко А. Я. Обобщения закона Мура // Информатика и кибернетика. 2017. № 3. С. 14—23.

© Ситник А. А., 2019

* Ситник Александр Александрович, кандидат юридических наук, доцент, доцент кафедры финансового права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА) aasitnik@gmail.com
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

щей силой цифровой экономики. В связи с этим можно говорить о том, что экономика начала приобретать цифровой характер в последнее десятилетие.

Современное общество находится только в самом начале пути формирования цифровой экономики. Особенностью текущего этапа развития цифровой экономики является не только внедрение уже существующих, но и осознание потенциала новых технологий (например, технологий больших данных (Big Data), нейротехнологий, технологии блокчейн, роботизации и т.д.). Таким образом, можно прогнозировать, что в ближайшее время общественные отношения, связанные с использованием цифровых технологий, получат свое дальнейшее развитие. Это, в свою очередь, рождает новые, зачастую трудноразрешимые вызовы для права как инструмента регулирования общественных отношений нового типа и для юридической науки, призванной выполнять прогностическую функцию, связанную с оценкой рисков внедрения новых технологий и выработкой эффективных подходов к их правовому регулированию.

Согласно традиционному пониманию, финансы как экономическая категория представляют собой совокупность экономических отношений, связанных с аккумулярованием, распределением (перераспределением) и использованием фондов денежных средств, а также контролем за их использованием. Финансовые отношения являются видом экономических отношений. В связи с этим цифровые технологии, воздействуя на экономику, влияют и на финансовое право (цифровые технологии → экономика → финансовое право).

Говоря о финансовом праве в условиях цифровизации экономики, следует отметить, что новые технологии, с одной стороны, ведут к расширению предмета правового регулирования (например, рассматриваемая отрасль стала регулировать общественные отношения, складывающиеся в процессе обращения электронных денег), а с другой — являются инструментом, способствующим регулированию, администрированию, финансовому контролю и надзору.

Технологии, применяемые в рамках финансовых отношений, общераспространенно именуются финансовыми технологиями. В настоящее время финансовые технологии (FinTech) рассматриваются не просто как разрозненные методы и инструменты, способствующие оказанию финансовых услуг, но как отдельная отрасль экономики, состоящая из организаций, производящих особый вид продукции — финансовые технологии. Таким образом, FinTech можно рассматривать и как отдельные технологии, и как отрасль экономики.

На сегодняшний день существует несколько классификаций финансовых технологий. Так, например, группа немецких авторов предлагает выделять финансовые технологии, связанные:

- 1) с финансированием (краудфандинг, кредит и факторинг);
- 2) управлением активами (социальный трейдинг, автоматизированные системы консультирования, управление личными финансами, инвестирование и банкинг);
- 3) платежами (альтернативные платежные методы, блокчейн и криптовалюты);
- 4) другими финансовыми технологиями в сфере страхования³.

Очевидно, что данная классификация отражает, хотя и неполно, сектора финансового рынка, на которых применяются соответствующие технологии.

Кроме того, предлагается разграничивать финансовые технологии:

1. Регулирующие технологии (RegTech) — применяются организациями, осуществляющими деятельность на финансовом рынке, для оптимизации процессов, связанных с выполнением регуляторных и надзорных требований.

В частности, Банк России среди регулирующих технологий выделяет:

- технологии комплаенс-контроля — направлены на обеспечение соблюдения регуляторных и надзорных требования, в том числе для выявления и управления рисками, автоматизации процессов раскрытия информации и т.д.;
- технологии идентификации — связаны с проверкой клиентов и иных лиц, участвующих

³ Dorfleitner G., Hornuf L., Schmitt M., Weber M. FinTech in Germany. Springer International Publishing AG, 2017. P. 7.

- в денежных операциях, в том числе при первичном приеме на обслуживание, а также последующей идентификации в процессе совершения указанных операций в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения;
- технологии мониторинга транзакций — имеют своей целью выявление отклонений и нарушений в процессах, связанных с переводом денежных средств, валютными операциями, а также операциями с финансовыми инструментами;
 - технологии управления рисками — направлены на автоматизацию управления рисками (рыночными и операционными). В отношении рыночных рисков данные технологии предполагают автоматизацию оценки финансовых инструментов, операций с денежными средствами, контроля установленных лимитов и т.д., а применительно к операционным рискам позволяют повысить эффективность внутренних процедур, обеспечить защиту от мошеннических действий и т.д.;
 - технологии, связанные с отчетностью — формируют и предоставляют отчетность в автоматическом режиме, позволяя тем самым снизить расходы на эксплуатацию информационных систем⁴.

Таким образом, в разработке, внедрении и развитии RegTech в первую очередь заинтересованы хозяйствующие субъекты, поскольку эти технологии позволяют, с одной стороны, снизить издержки (за счет уменьшения расходов на администрирование информационных систем, сокращения персонала, а также ускорения процедур контроля), а с другой — обеспечить соблюдение предъявляемых государством требований. Исходя из этого, можно сделать вывод, что движущей силой развития RegTech является рынок. Успешность той или иной регулирующей

технологии зависит от качества и стоимости предлагаемых решений.

2. Надзорные технологии (SupTech) — внедряются в практику органов регулирования и надзора на финансовых рынках для повышения эффективности данной деятельности. Такие технологии связаны с автоматической обработкой отчетности и иной информации, поступающей от субъектов финансового рынка, с мониторингом и анализом рыночных и операционных рисков, цифровизацией регуляторных требований (разработка сервисов, позволяющих субъектам финансового рынка оперативно выявлять изменения в указанных требованиях и применять их в своей практике), и т.д. Развитие SupTech, как отмечает Банк России, «полностью зависит от нацеленности регуляторов на модернизацию подходов в сфере регулирования и надзора»⁵.

Из всего вышесказанного можно сделать ряд выводов:

- во-первых, деление RegTech и SupTech происходит в зависимости от субъектов, которые внедряют соответствующие технологии в свою деятельность: участники финансового рынка или регулятор (Банк России). В то же время они, по сути, направлены на одно и то же — обеспечение законности на финансовых рынках. Сам термин «регулирующие технологии» следует признать неудачным: такие технологии не являются регулирующими по своей сути. Регулирование — процесс целенаправленного воздействия на общественные отношения. RegTech не влияют на общественные отношения, их применение, как уже было сказано, имеет своей целью обеспечить соблюдение регуляторных требований. Таким образом, то, что сейчас принято называть «регулирующими технологиями», по сути, также является надзорными технологиями, но внедряемыми хозяйствующими субъектами;

⁴ Доклад для общественных консультаций «Вопросы и направления развития регуляторных и надзорных технологий (RegTech и SupTech) на финансовом рынке в России». С. 6—7.

⁵ Доклад для общественных консультаций «Вопросы и направления развития регуляторных и надзорных технологий (RegTech и SupTech) на финансовом рынке в России». С. 7.

— во-вторых, Банк России выделяет RegTech и SupTech только применительно к сектору финансового рынка. В то же время, на наш взгляд, данный подход чрезвычайно узкий. Практика свидетельствует о том, что инновационные цифровые технологии используются во всех областях финансового права. Например, в рамках налогового контроля в последнее время внедрены различные цифровые сервисы (личный кабинет налогоплательщика, сервисы проверки сведений о контрагентах и т.д.), автоматизированные информационные системы (например, автоматизированная система контроля (АСК «НДС») и т.д. Цифровые технологии широко используются и в рамках бюджетных правоотношений: введены в эксплуатацию информационная система управления общественными финансами «Электронный бюджет», Государственная информационная система о государственных и муниципальных платежах⁶, Государственная автоматизированная информационная система «Управление», Система удаленного финансового докумен-

тооборота (СУФД-online) и т.д. Названные технологии могут быть квалифицированы как финансовые, поскольку либо непосредственно связаны с публичными финансами, либо используются для целей финансово-правового регулирования общественных отношений.

Кроме того, ряд технологий, рассматриваемых в качестве финансовых, связан не только с финансовым рынком. В качестве примера можно привести технологии идентификации клиентов в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения, которые со всей очевидностью затрагивают не только финансовые рынки.

Таким образом, можно заключить, что, в узком понимании финансовые технологии — это совокупность инструментов и методов, применяемых исключительно на финансовых рынках, а в широком — технологий, используемых во всех областях, связанных с финансовым регулированием, контролем и надзором.

БИБЛИОГРАФИЯ

1. Антропченко А. Я. Обобщения закона Мура // Информатика и кибернетика. — 2017. — № 3. — С. 14—23.
2. Dorfleitner G., Hornuf L., Schmitt M., Weber M. FinTech in Germany. — Springer International Publishing AG, 2017. — 121 p.

Материал поступил в редакцию 6 мая 2019 г.

⁶ На основании ч. 1 ст. 21.3 Федерального закона от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» государственная информационная система о государственных и муниципальных платежах является информационной системой, предназначенной для размещения и получения информации об уплате физическими и юридическими лицами платежей за оказание государственных и муниципальных услуг, услуг, указанных в ч. 3 ст. 1 и ч. 1 ст. 9 данного Федерального закона, иных платежей, являющихся источниками формирования доходов бюджетов бюджетной системы Российской Федерации (за исключением платежей, являющихся источниками формирования доходов бюджетов бюджетной системы Российской Федерации, перечень которых устанавливается в соответствии с бюджетным законодательством Российской Федерации), а также иных платежей, в случаях, предусмотренных федеральными законами.

FINANCIAL TECHNOLOGIES: THE CONCEPT AND TYPES

SITNIK Aleksandr Aleksandrovich, PhD in Law, Associate Professor of the Department of Financial Law of Kutafin Moscow State Law University (MSAL)
aasitnik@gmail.com
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

Abstract. *The article is devoted to the study of the influence of digital economy on financial law. It is determined that in the context of economy digitalization, new technologies, on the one hand, lead to the expansion of the subject of legal regulation, and, on the other hand, they represent a tool that promotes regulation, administration, financial control and supervision. The paper discusses various types of financial technologies, primarily regulatory (RegTech) and supervisory (SupTech) ones. According to the results of the study, the author concludes that the term regulatory technologies is generally inappropriate. In addition, it should be said that, in a narrow sense, financial technology provides for a set of instruments and methods used exclusively in financial markets and, in broad terms, used in all areas related to financial regulation, control and supervision.*

Keywords: *financial technologies, regulatory technologies, supervisory technologies, financial law, finance.*

REFERENCES (TRANSLITERATION)

1. *Antropchenko A. Ya. Obobshcheniya zakona Mura // Informatika i kibernetika. — 2017. — № 3. — S. 14—23.*

БАНКОВСКАЯ СИСТЕМА И БАНКОВСКАЯ ДЕЯТЕЛЬНОСТЬ

В. М. Камалян*

Правовые риски использования цифровых технологий в банковской деятельности¹

***Аннотация.** В работе автор на основе анализа правовых рисков использования смарт-контрактов в банковской деятельности делает вывод о необходимости специального правового регулирования использования цифровых технологий в банковской деятельности, которое позволило бы минимизировать рассмотренные правовые риски. Автор полагает, что подобное правовое регулирование в целях минимизации правовых рисков должно определять смарт-контракт не как конструкцию договора, заключенного в письменной форме, а как способ исполнения обязательств. Анализируя правовые риски, связанные с идентификацией личности при внедрении цифровых технологий в банковскую деятельность, автор предлагает использование блокчейн-технологии как основу системы идентификации клиентов, при этом используя исключительно преимущественные возможности данной технологии с соблюдением требований международных стандартов и национального законодательства о противодействии отмыванию доходов, полученных преступным путем, и финансированию терроризма. Данное решение позволит упростить и защитить систему идентификации и обработки данных о клиентах банков, однако оно требует эффективной государственной поддержки и правового регулирования.*

***Ключевые слова:** цифровые технологии, финансовые технологии, цифровизация, цифровой банкинг, правовые риски, смарт-контракт, правовая природа смарт-контракта, блокчейн, идентификация, отмывание преступных доходов, финансирование терроризма.*

DOI: 10.17803/1994-1471.2019.103.6.032-039

Банковская деятельность является самым динамично развивающимся сегментом экономики. Одним из способов развития банковского рынка является широкое внедрение в деятельность кредитных организаций

новых банковских технологий. В условиях активной цифровизации, связанной с появлением новых финансовых технологий, открываются новые перспективы использования цифровых технологий в банковской деятельности, позво-

¹ Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16203 мк на тему «Российское и зарубежное право об использовании цифровых технологий в банковской деятельности и практика его применения: сравнительно-правовой аспект».

© Камалян В. М., 2019

* Камалян Владислав Михайлович, аспирант Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
vladkamalyan@mail.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

ляющие решать ряд важных как для кредитной организации, так и для ее клиентов задач:

- снижение операционных расходов банка и его клиента;
- повышение скорости совершения операций;
- снижение трудоемкости процессов совершения банковских операций;
- минимизация банковских рисков;
- повышение прозрачности совершения операций и рост уровня доверия к кредитным организациям;
- повышение качества обслуживания клиентов.

Подобного рода задачи постоянно возникают перед кредитными организациями. Когда появляется технология, которая позволяет в определенной мере решить данные задачи, любой банк должен быть заинтересован в ее внедрении в банковскую деятельность. Однако кредитная организация также должна осознавать, с какими правовыми рисками она может столкнуться при внедрении цифровых технологий. Поэтому необходимо постоянно анализировать подобные риски и искать пути их минимизации. Одними из самых существенных правовых рисков внедрения цифровых технологий в банковскую деятельность являются риски, связанные с использованием смарт-контракта, а также риски проблемной идентификации клиента.

1. ПРАВОВЫЕ РИСКИ ИСПОЛЬЗОВАНИЯ СМАРТ-КОНТРАКТА В БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ

Технология смарт-контракта является совершенно новой для всего мира, и ее появление тесно связано с активным развитием блокчейн-технологий. Разумеется, на такое развитие не могут не реагировать как представители государственной власти разных государств, так и представители научных и банковских сообществ. В российском банковском праве пока отсутствует упоминание о смарт-контрактах, а теоретическая концепция внедрения данного понятия в правовую систему

еще основательно не разработана. Вместе с тем цифровизация банковской деятельности определенно требует разработки доктринальной концепции смарт-контрактов, в рамках которой необходимо выявить правовые риски использования смарт-контрактов в банковской деятельности. Смарт-контракт можно определить как программный код, полностью или частично отражающий и автоматически исполняющий заключенный между участниками договор на базе технологии распределенного реестра данных.

Рассмотрим правовые риски использования смарт-контракта на следующем примере. Британский банк Barclays использовал смарт-контракты для проведения сделок с аккредитивами в рамках международной поставки товаров (сыра и сливочного масла). В состав документов, подтверждающих исполнение условий аккредитива, вошли электронные документы: сертификат происхождения товара, страховой сертификат, счет, товарно-транспортная накладная². Стоит отметить, что подробности данной сделки и особенности ее оформления публично неизвестны, поскольку составляют коммерческую тайну сторон. Поэтому нижеследующие суждения не следует применять к фактической стороне данной сделки.

Если смарт-контракт считать договором, то в данном случае смарт-контракт может представлять собой как минимум основной договор между поставщиком и покупателем, но также может являться и смешанным договором, включающим в себя следующие элементы: основной договор между поставщиком и покупателем, договор между покупателем и банком-эмитентом о выдаче аккредитива, договор между банком-эмитентом и исполняющим банком, содержащий полномочие совершить платеж. Кроме того, допустимо заключать несколько смарт-контрактов на исполнение отдельных указанных выше обязательств по основному договору и аккредитиву.

В рамках данной операции возможны следующие правовые риски.

² Аналитический обзор Центрального Банка РФ по теме «Смарт-контракты» от октября 2018 г. С. 10 // Сайт Центрального Банка РФ. URL: http://www.cbr.ru/content/document/file/47862/smartkontrakt_18-10.pdf (дата обращения: 23.03.2019).

Во-первых, смарт-контракт — технологически сложное явление, представляющее собой программный код, написанный на языке компьютера. Поэтому для составления смарт-контракта всегда привлекается специалист, имеющий достаточную техническую квалификацию. Такой специалист едва ли владеет юридической техникой, чтобы всегда верно отражать действительную юридическую волю сторон в программном коде. Поэтому с первым правовым риском использования смарт-контракта стороны сталкиваются уже на стадии его составления: специалист, не обладающий юридическим образованием, не всегда способен в точности отразить юридическую волю сторон по сделке. В итоге исполнение смарт-контракта может привести к иным результатам, вопреки воле сторон. Например, специалист может не придать должного значения товарно-транспортным накладным и не включить условия о получении программой данных об этом документе в смарт-контракт. Как следствие, покупатель не получает данные о товарно-транспортной накладной, которая является важным документом бухгалтерской отчетности. Впоследствии покупателю необходимо дополнительно запрашивать у поставщика документы, что занимает определенное время и требует определенных расходов.

Второй существенный правовой риск использования смарт-контракта заключается в возможности технической ошибки, допущенной специалистом при составлении смарт-контракта. Любая техническая ошибка в коде, будь это даже пропущенный символ или цифра, способна привести к неправильному ходу исполнения смарт-контракта или даже к полной остановке, сбою. Запущенный смарт-контракт невозможно изменить, исправить или дополнить ввиду особенностей его технической природы, построенной на технологии блокчейн³. Поэтому код, заложенный в смарт-контракт, должен быть технически идеален, чтобы программа смогла

произвести алгоритм действий от начала до самого конца.

В случае ошибки хода смарт-контракта стороны могут столкнуться со следующими правовыми проблемами. В первую очередь это неисполнение обязательства стороны. В указанном выше примере допускаем, что ввиду ошибки в смарт-контракте деньги не поступили на счет бенефициара (поставщика), то есть покупатель, хотя и не преднамеренно, не исполнил обязательство по оплате товара. Поставщик в таком случае будет предъявлять требования именно к покупателю⁴, несмотря на вину специалиста, допустившего техническую ошибку при составлении смарт-контракта. Покупатель оказывается в такой ситуации, что должен оплатить полученный товар другим путем. Более того, если денежные средства были также заложены в смарт-контракт и заблокированы им, покупателю придется искать новые финансовые возможности, чтобы погасить образовавшуюся задолженность, при этом претерпев убытки в размере заблокированных денежных средств. Поэтому в данном случае стороны могут нести не только правовые, но и финансовые риски.

Третий немаловажный правовой риск связан с ситуацией возникновения споров между сторонами. Смарт-контракт способен минимизировать вероятность возникновения споров ввиду автоматизации исполнения обязательства, но свести к нулю такую вероятность теоретически невозможно. Тем не менее, продолжая ситуацию с неисполнением покупателем обязательств по оплате товара, дополним ее следующими условиями: поставщик обратился в суд с требованием взыскать денежные средства. Суд запросит договор, на основании которого возник спор. И в данном случае ситуация имеет два направления развития в зависимости от того, считать ли смарт-контракт непосредственно договором⁵. Если его считать таковым, то поставщику необходимо будет предоставить

³ *Ефимова Л. Г., Сиземова О. Б.* Правовая природа смарт-контракта // *Банковское право.* 2019. № 1. С. 24.

⁴ *Савельев А. И.* Некоторые правовые аспекты использования смарт-контрактов и блокчейн-технологий по российскому праву // *Закон.* 2017. № 5. С. 102.

⁵ *Городов О. А., Егорова М. А.* Основные направления совершенствования правового регулирования в сфере цифровой экономики в России // *Право и цифровая экономика.* 2018. № 1 (01). С. 9.

смарт-контракт суду. Однако единственное, что он сможет предоставить, — это код смарт-контракта. Судья — человек с юридическим образованием, не сведущий в программировании, — не сможет принять текст кода как надлежащее доказательство основания спорных взаимоотношений⁶. Поставщик в таком случае оказывается в ситуации, что он фактически ничего не может предоставить суду в подтверждение заявленных доводов. Суд потребует надлежащую письменную форму договора, в противном случае истца ждет отказ в удовлетворении исковых требований. Таким образом, поставщик оказывается лишенным правовой защиты. Ситуация складывается иначе, если смарт-контракт считать не договором, а лишь средством его исполнения. В таком случае наряду со смарт-контрактом составляется обычный письменный договор, который закрепляет волю сторон на человеческом языке, понятном как для самих сторон, так и для судьи. Следовательно, интересы потерпевшей стороны всегда будут защищены в суде. Таким образом, данный правовой риск возможно и необходимо избегать путем заключения обычного письменного договора.

Стоит отметить, что данный способ позволит минимизировать и ранее указанные риски. В частности, обычный письменный договор можно предоставить специалисту для удобства составления смарт-контракта, и тогда текст будет в максимальной степени коррелировать с программным кодом. Таким образом, риск неправильного отражения воли сторон в смарт-контракте минимизируется за счет письменного отражения воли сторон на бумажном носителе.

Более того, обычный письменный договор позволит минимизировать правовые и финансовые риски, возникающие при неправильном ходе исполнения смарт-контракта: представляется, что помимо основного договора поставки необходимо заключать договор со специалистом, который будет составлять смарт-контракт и, самое главное, нести ответственность за неправильное его составление. В случае, когда из-за технической ошибки смарт-контракт не

исполнил обязательство покупателя по оплате товара, вина лежит на специалисте и ответственность нести должен тоже он. В случае если специалист является штатным сотрудником одной из сторон, конечно, ответственность будет нести та сторона, в штате которой данный специалист работает.

Более того, как уже отмечалось, условия смарт-контракта невозможно поменять или отменить. Можно предполагать, что нормы гражданского права об изменении и о расторжении договора неприменимы к смарт-контракту. Поэтому представляется, что это было бы грубым нарушением принципов гражданского права, в связи с чем нельзя приравнивать смарт-контракт к договору. Отсюда вытекает еще один правовой риск использования смарт-контракта, связанный с возможностью изменения или отмены смарт-контракта, если, предположим, смарт-контрактом была исполнена противоправная сделка. Например, покупатель приобрел квартиру в ипотеку у собственника без согласия супруги последнего. Смарт-контракт выполнил следующие действия: перечислил кредитные денежные средства банка на счет заемщика-покупателя и затем, получив данные об успешной регистрации нового права собственности на квартиру, перевел денежные средства плательщика на счет продавца. Возникает необходимость в реституции прав сторон, но как это сделать, если процесс смарт-контракта необратим и его невозможно изменить? Представляется, что существует два варианта реституции прав в данной ситуации: традиционный или посредством смарт-контракта. При традиционном варианте реституция денежных обязательств происходит посредством традиционных форм расчетов: продавец возвращает деньги покупателю, покупатель возвращает ипотечный кредит банку. Регистрационная запись о праве собственности на квартиру на основании решения суда отменяется Росреестром, что восстанавливает права прежнего собственника на квартиру. Обратные действия можно также совершить в добровольном порядке посредством уже нового смарт-контракта, аналогичного пре-

⁶ Савельев А. И. Указ. соч. С. 94—117.

дыдущему, но уже с другими сторонами — плательщиком и получателем.

Таким образом, с правовой точки зрения крайне опасно считать смарт-контракт договором: чтобы все стороны имели правовую защиту своих интересов, необходимо традиционное письменное заключение договора, причем не только основного, но и с составителем смарт-контракта. Поэтому признание смарт-контракта договором является фактором, приводящим к росту правовых рисков использования данной технологии в банковской деятельности. В связи с этим необходимо законодательно установить, что смарт-контракт не является договором, заключенным в письменном виде, не отражает волю сторон и является лишь инструментом исполнения обязательств. Тогда и практика применения смарт-контракта, и правоприменительная практика не будут двойственными, что позволит более эффективно внедрять данную технологию в банковскую деятельность.

2. ПРАВОВЫЕ РИСКИ ИДЕНТИФИКАЦИИ В ЦИФРОВОМ БАНКИНГЕ

Современная банковская деятельность базируется на основополагающем принципе KYC (Know Your Client — Знай своего клиента), значение которого состоит в идентификации банком клиентов, а также бенефициаров банковских операций. Данный принцип сформулирован как в Международных стандартах по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения, принятых ФАТФ⁷, так и во многих национальных правовых системах, в частности в России — в Федеральном законе от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов,

полученных преступным путем, и финансированию терроризма»⁸, а также в Положении об идентификации кредитными организациями клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (утв. Банком России 15.10.2015 № 499-П)⁹. Основная задача данного принципа — это борьба с легализацией преступных доходов и финансированием терроризма. При внедрении цифровых технологий в банковскую деятельность важно не допустить нарушения данных принципов. Опасения в данном случае совсем не безосновательны по следующим причинам.

Если говорить о внедрении такой технологии, как блокчейн, то стоит отметить, что блокчейн основан на полной анонимности: стороны транзакций не знают друг о друге ничего, кроме того, что они передают друг другу. К сожалению, сегодня блокчейн уже активно применяется и в противоправных целях. Существует так называемый даркнет (DarkNet), базирующийся на технологии блокчейн, где участники могут совершенно легко и, главное, анонимно приобрести оружие, наркотики, поддельные документы и много другое. Все транзакции происходят через криптовалюту, отследить участников сделки практически невозможно благодаря асимметричному шифрованию. Данный пример показывает, как блокчейн уже способствует развитию легализации преступных доходов и финансированию терроризма. Поэтому возникает вопрос, как банку внедрить блокчейн в свое программное обеспечение, чтобы не нарушать законодательство о противодействии легализации преступных доходов и финансированию терроризма. Именно данный риск является существенным правовым

⁷ П. 10 Раздела D Рекомендаций ФАТФ Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения — Перевод подготовлен Международным учебно-методическим центром по финансовому мониторингу, Вече, 2012 — Опубликовано на сайте Росфинмониторинга <http://www.fedsfm.ru/content/files/documents/fatf/рекомендации%20фатф.pdf>, дата обращения: 23.03.2019 г.

⁸ Российская газета. № 151—152. 09.08.2001.

⁹ Вестник Банка России. № 115. 16.12.2015.

риском внедрения технологии блокчейн в банковскую деятельность.

Таким образом, банкам необходимо найти определенный компромисс между преимуществами блокчейна и требованиями законодательства, чтобы эффективно применять данную технологию.

В частности, таким компромиссом является включение блокчейн-технологии в процесс идентификации, точнее — перевод процесса идентификации на блокчейн-технологии. Необходимо разработать и законодательно утвердить систему идентификации личности, основанную на блокчейне, где все данные личности будут оцифрованы и зашифрованы, вследствие чего защищены. Посредством блокчейна данные могут передаваться в том числе банку, причем моментально и комплексно. Стоит отметить, что такая система позволит защитить персональные данные клиента, не допустив незаконной утечки или передачи данных, поскольку система децентрализована и асимметрично зашифрована. Сегодня на частном уровне уже разрабатываются подобные системы.

Так, например, модель Civic позволяет (в случае возникновения такой необходимости) обеспечить безопасный и более дешевый доступ к проверке подлинности личности с помощью блокчейн-технологии. Проверку личной информации больше не нужно будет проходить заново каждый раз, когда требуется регистрация в новом приложении или сайте. И все это без фактического сбора и хранения пользовательской информации со стороны компании. Блокчейн здесь используется для защиты данных. Эти данные по всей строгости проверены Civic или другими партнерскими системами идентификации, а затем засвидетельствованы и привязаны к блокчейну в виде данных, не поддающихся дешифровке. Эти данные обмениваются исключительно между пользователем и определенным контрагентом с помощью Civic tokens (CVC). Участниками сети могут быть банки, финансовые сервисы, организации сферы здравоохране-

ния и другие надежные организации. Civic уже имеет рабочий продукт проверки подлинности, который доступен во всем мире и получил премию «Лучший новый стартап» на конференции «Идентификация пользователей» в 2017 г.¹⁰

uPort — еще одно решение для управления идентификацией, разработанное престижной компанией Blockchain ConsenSys. Главная цель разработчиков uPort — создание элементарной в использовании системы идентификации личности на базе блокчейна Эфириум. Система uPort рассматривает мобильный телефон человека как продолжение его собственного «я». Во время первичной настройки системы с вашего разрешения она извлекает данные из телефона и записывает смарт-контракт на их основе. В дальнейшем им можно пользоваться по мере необходимости.

Данная платформа в конце 2017 г. стала доступна не отдельно взятому лицу, а целому городу. Речь идет о швейцарском Цуге, именуемом «Криптодолиной». Вот уже несколько месяцев реализуется программа регистрации удостоверений для жителей города на основе блокчейна. Это позволит людям получить доступ к электронным услугам, таким как подтверждение проживания и онлайн-голосование. Система должна ознаменовать собой новую ветвь развития блокчейна, поскольку она демонстрирует, что с помощью данной технологии городское правительство может осуществлять цифровую проверку граждан¹¹.

Таким образом, технология блокчейн представляет собой как риск возникновения проблемы идентификации клиентом банка, так и решение данной проблемы. Стоит отметить, что сегодня идентификация клиента основана на государственных и международных стандартах. Поэтому до тех пор, пока блокчейн-технологии не будут законодательно одобрены для целей идентификации как на государственном, так и на международном уровне, банки не рискнут менять систему идентификации самостоятельно.

¹⁰ Системы идентификации личности на базе блокчейна. 24.02.2018 // URL: <https://cryptogu.ru/sistemy-identifikacii-lichnosti-na-baze-blokchejna/> (дата обращения: 23.03.2019).

¹¹ Системы идентификации личности на базе блокчейна.

Таким образом, можно сделать следующие выводы:

1. Внедрение цифровых технологий в банковскую деятельность требует специального правового регулирования с целью минимизации правовых рисков их использования.

2. В целях минимизации правовых рисков смарт-контракт не стоит приравнивать к договору: данная технология является лишь средством исполнения обязательств.

3. Правовые риски использования смарт-контракта во многом связаны с лицом, осуществляющим разработку смарт-контракта, в связи

с чем необходимо установить правовой статус и ответственность такого лица.

4. Правовые риски идентификации личности в банковской деятельности могут быть минимизированы за счет внедрения цифровых технологий в правильное русло.

5. Внедрение цифровых технологий в банковскую деятельность требует особой государственной поддержки в рамках эффективного правового регулирования, позволяющего сочетать пользу цифровых технологий и публичные интересы государства.

БИБЛИОГРАФИЯ

1. *Городов О. А., Егорова М. А.* Основные направления совершенствования правового регулирования в сфере цифровой экономики в России // *Право и цифровая экономика*. — 2018. — № 1 (01). — С. 6—11.
2. *Ефимова Л. Г., Сиземова О. Б.* Правовая природа смарт-контракта // *Банковское право*. — 2019. — № 1. — С. 21—27.
3. *Савельев А. И.* Некоторые правовые аспекты использования смарт-контрактов и блокчейн-технологий по российскому праву // *Закон*. — 2017. — № 5. — С. 94—117.

Материал поступил в редакцию 6 мая 2019 г.

LEGAL RISKS OF USING DIGITAL TECHNOLOGIES IN BANKING¹²

KAMALYAN Vladislav Mikhailovich, Postgraduate Student of the Kutafin Moscow State Law University (MSAL)
vladkamalyan@mail.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

Abstract. *Based on the analysis of legal risks of using smart contracts in banking activities, the author concludes that there is a need for special legal regulation of the use of digital technologies in banking, which would minimize the legal risks examined in the paper. The author believes that such legal regulation in order to minimize legal risks should define a smart contract as a way of fulfillment of obligations rather than as a design of a contract concluded in writing. Analyzing the legal risks associated with the person identity during the introduction of digital technologies in banking, the author suggests the use of blockchain technology as the basis of the system of identification of customers using exclusively the advantages of this technology in compliance with the requirements of international standards and national legislation regulating counteraction to laundering of proceeds of crime and financing of terrorism. This solution will simplify and protect the system of identification and processing of data regarding the clients of banks, but it requires effective state support and legal regulation.*

¹² The research was carried out with the financial support of RFBR within the framework of the scientific project No. 18-29-16203 mk on the topic «Russian and Foreign Law on the Use of Digital Technologies in Banking and the Practice of its Application: Comparative Law Aspect».

Keywords: *digital technologies, financial technologies (fintech), digitalization, digital banking, legal risks, smart contract, legal nature of a smart contract, blockchain, identification, laundering of proceeds of crime, financing of terrorism.*

REFERENCES (TRANSLITERATION)

1. *Gorodov O. A., Egorova M. A. Osnovnye napravleniya sovershenstvovaniya pravovogo regulirovaniya v sfere cifrovoj ekonomiki v Rossii // Pravo i cifrovaya ekonomika. — 2018. — № 1 (01). — S. 6—11.*
2. *Efimova L. G., Sizemova O. B. Pravovaya priroda smart-kontrakta // Bankovskoe pravo. — 2019. — № 1. — S. 21—27.*
3. *Savel'ev A. I. Nekotorye pravovye aspekty ispol'zovaniya smart-kontraktov i blokchejn-tehnologij po rossijskomu pravu // Zakon. — 2017. — № 5. — S. 94—117*

ГРАЖДАНСКОЕ И СЕМЕЙНОЕ ПРАВО

И. З. Аюшеева*

Особенности гражданско-правового регулирования отношений по предоставлению в пользование недвижимого имущества в условиях развития экономики совместного потребления (sharing economy)¹

***Аннотация.** В настоящее время развиваются отношения цифровой экономики, в условиях четвертой промышленной революции происходит изменение их регулирования. В то же время проблемы экологии и ограниченные ресурсы постепенно меняют отношение к культуре потребления: наметилась тенденция перехода от потребительского общества к экономике совместного потребления (sharing economy), характеризующейся коллективным использованием товаров и услуг. Эти тенденции проявляются в различных сферах, в том числе в сфере владения и пользования недвижимым имуществом, в частности жилыми помещениями. В настоящее время появляются различные сервисы, например Airbnb, которые позволяют предоставлять недвижимое имущество в пользование, развивается формат совместного пользования офисными помещениями (коворкинг). Актуальным является определение природы договоров, которые возникают между пользователями и владельцами сервисов, а также непосредственно между пользователями, установление прав и обязанностей сторон, объема их ответственности, что требует более подробного изучения обозначенной проблемы.*

***Ключевые слова:** недвижимое имущество, совместное пользование жильем, договор, аренда, коммерческий наем, смарт-контракт, экономика совместного потребления, цифровая экономика, непоименованный договор, гражданско-правовая ответственность.*

DOI: 10.17803/1994-1471.2019.103.6.040-048

¹ Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16054 «Концептуальные основы правового регулирования отношений по коллективному использованию товаров и услуг (sharing economy) в условиях развития цифровых технологий».

© Аюшеева И.З., 2019

* Аюшеева Ирина Зориктуевна, кандидат юридических наук, доцент кафедры гражданского права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
aiusheeva@gmail.com
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

В настоящее время общество постепенно осознает, что ресурсы планеты ограничены, а экологические проблемы являются глобальными и их разрешение должно носить приоритетный характер для обеспечения безопасности и возможности дальнейшего существования всего человечества. Ограниченность ресурсов меняет отношение к культуре потребления: наметилась тенденция перехода от потребительского общества к экономике совместного потребления (sharing economy), характеризующейся совместным (коллективным) использованием товаров и услуг. Эти тенденции в наши дни проявляются в различных сферах (совместное пользование недвижимым имуществом, в том числе хоумшеринг, движимыми вещами, в том числе каршеринг, и т.п.). Современные технологии, позволяющие совершать сделки в электронной форме и исполнять договоры без участия человека (смарт-контракты), дали идее шеринга новое развитие, облегчая задачу соединения большого количества незнакомых друг другу людей.

Р. Ботсман отмечала, что «люди начинают осознавать способность технологии выявлять простаивающие мощности и максимизировать пользу от различных видов активов, от навыков до недвижимости и материальной собственности, в масштабах и способами, которые до этого были просто невозможны. Это экономика и культура, получившая название «совместное потребление»². Совместное потребление рассматривается как новая культура и новая социоэкономическая модель общественных отношений, в рамках которой признается преимущество модели временного пользования объектом, находящимся в общем доступе или принадлежащим другому лицу и бывшим в употреблении ранее, над приобретением нового

объекта в собственность. Данная модель способна изменить бизнес, потребительское поведение и стиль нашей жизни в целом³.

На современном этапе самыми популярными сферами экономики совместного потребления признаются каршеринг и сервисы аренды жилья, за экономикой совместного потребления (коллективного использования, sharing economy) видится будущая модель экономических отношений. Как отмечают в своих исследованиях экономисты, в России концепция совместного потребления приобретает популярность в последние 5—7 лет, уже активно используются такие ресурсы, как OtdamDarom.ru (darom.org), ДаруДар, YouDo, BeepCar, BlaBlaCar, Делимобиль и др.⁴

Указанные выше факторы делают актуальной необходимость осмысления особенностей гражданско-правового регулирования отношений экономики совместного потребления, определения договорных конструкций, опосредующих данные отношения, их природы, особенностей субъектного состава, содержания, а также особенностей осуществления прав и обязанностей, ответственности сторон. В настоящей статье рассматриваются особенности гражданско-правового регулирования отношений по предоставлению в пользование недвижимого имущества, прежде всего жилых помещений, в условиях развития экономики совместного потребления.

На современном этапе существуют разные модели организации договорных связей в рамках экономики совместного потребления. В рамках одной модели отношений экономики совместного потребления участником возникших договорных отношений с пользователями выступает компания — владелец маркетплейса. Другая модель предполагает установление обязательственных отношений между собствен-

² Botsman R. The currency of the new economy is trust // TED. URL: https://www.ted.com/talks/rachel_botsman_the_currency_of_the_new_economy_is_trust?referrer=playlist-the_economy_of_trust (дата обращения: 21.11.2018).

³ См.: Botsman R., Rogers R. What's Mine Is Yours: The Rise of Collaborative Consumption // HarperBusiness, 2010. P. X—XXII.

⁴ Головецкий Н. Я., Гребенюк В. В. Фундаментальные основы экономики совместного потребления // Вестник Московского университета имени С. Ю. Витте. Серия 1 : Экономика и управление. 2017. № 4. С. 21—22.

ником и пользователем, а в рамках третьей модели предполагается согласование интересов собственников имущества либо членов определенных сообществ, например собственников недвижимости.

Чуть более 10 лет назад был создан крупнейший маркетплейс для людей, путешествующих по всему миру, — Airbnb.com, пользователи которого обычно преследуют цель получить доход от своего имущества, не используемого в настоящее время, а также встретить новых людей и расширить круг общения⁵. Онлайн-платформу GETset называли Airbnb для кинопроизводителей (на данной платформе были представлены бюджетные съемочные площадки местных владельцев, которые можно арендовать)⁶. Площадка TalkTalkbnb предлагает свободный языковой обмен и возможность найти жилье и еду (по сути, это маркетплейс бесплатного жилья для путешественников, готовых поговорить на родном языке, обмен деньгами между участниками не предусмотрен)⁷. Как отмечается, этот стартап занял нишу между сервисами, предлагающими бесплатное, но минимально удобное жилье, и проектами по модели Airbnb, использующими принцип «плати за комфорт»⁸. В настоящее время востребованы так называемые коворкинги, когда во временное пользование предлагают офисные помещения для совместной работы в одном пространстве, что минимизирует затраты на аренду для бизнесменов, фрилансеров, самозанятых граждан, позволяя им за небольшие деньги пользоваться всей инфраструктурой обычного офиса⁹.

Таким образом, идея совместного использования недвижимого имущества воплощена в различных моделях и опосредуется разны-

ми договорными конструкциями. Можно ли говорить о том, что возникающие в связи с совместным использованием жилых и нежилых помещений опосредующие договоры относятся к поименованным в законе договорным типам (аренды, найма жилого помещения, ссуды, возмездного оказания услуг и т.п.), являются ли они смешанными или обладают уникальными признаками, позволяющими отнести их к непоименованным договорам? Как отмечается в юридической литературе, решение насущных проблем правового регулирования отношений по совместному использованию недвижимого имущества возможно уже существующими юридическими инструментами, при этом, безусловно, юристы должны стремиться к тому, чтобы регулирование этой сферы менялось и развивалось, однако полагаться и ждать указанных изменений не имеет смысла, необходимо постепенно менять практику применения уже существующих договорных и иных юридических конструкций¹⁰.

Согласно п. 1.1 Условий предоставления услуг, размещенных на сайте Airbnb, платформа Airbnb — это онлайн-площадка, которая позволяет зарегистрированным пользователям и определенным третьим лицам, предлагающим услуги (пользователи и третьи лица, предлагающие услуги, именуются «хозяева», а предлагаемые ими услуги — «услуги хозяев»), публиковать объявления с предложением услуг хозяев на платформе Airbnb, а также общаться и совершать операции напрямую с пользователями, желающими забронировать данные услуги хозяев (пользователи, пользующиеся услугами хозяев, именуются «гости»). Услуги хозяев могут включать в себя сдачу в аренду мест для

⁵ *Botsman R., Rogers R. What's Mine Is Yours: The Rise of Collaborative Consumption* // HarperBusiness, 2010. P. XII; Airbnb.ru. URL: <https://www.airbnb.ru/terms> (дата обращения: 27.03.2019).

⁶ *Бидуэлл Дж. Это прорыв. 100 уроков бизнес-инноваций*. М.: Альпина Паблишер, 2019. С. 28—29.

⁷ *Бидуэлл Дж. Указ. соч.* С. 32; TalkTalkbnb. URL: <https://www.talktalkbnb.com/> (дата обращения: 27.03.2019).

⁸ *Бидуэлл Дж. Указ. соч.* С. 32—33.

⁹ См., например: *Workspace networking places*. URL: <http://wspace.space/rumyantsevo> (дата обращения: 01.04.2019); *Бизнес-коворкинг в Москва-Сити*. URL: <http://office24-7.ru/biznes-coworking> (дата обращения: 01.04.2019).

¹⁰ *Orsi J. Practicing law in the sharing economy: helping people build cooperatives, social enterprise, and local sustainable economies* // *Cooperative societies — Law and legislation — United States*. I. Title. 2012. P. 467.

проживания или иных помещений («жилье»), организацию одиночных или многодневных мероприятий в различных категориях («впечатления»), возможность доступа на уникальные мероприятия и территории («мероприятия»), а также иные услуги, связанные или не связанные с путешествиями. В пункте 1.2 Условий указано, что Airbnb предоставляет платформу Airbnb и не владеет, не создает, не продает, не перепродает, не контролирует, не предлагает, не предоставляет и не обеспечивает какие-либо объявления или услуги хозяев, а также не управляет ими, а также Airbnb не является организатором путешествий или продавцом туристических пакетов. Хозяева несут единоличную ответственность за свои объявления и услуги. Принимая или создавая бронирование, пользователи вступают в договорные отношения непосредственно друг с другом. Airbnb не является стороной или иным участником каких-либо договорных отношений между пользователями, а также не является агентом по недвижимости или страховщиком. Airbnb не выступает в качестве агента пользователей, за исключением случаев, предусмотренных Условиями¹¹.

Согласно п. 21.3 Условий, если страной проживания или постоянного местонахождения пользователя не является ни США, ни Китай, то настоящие Условия толкуются в соответствии с законодательством Ирландии. Применение Конвенции ООН о договорах международной купли-продажи товаров (КМКПТ) исключается. Выбор законодательства не влияет на права пользователя как потребителя в соответствии с нормами защиты прав потребителя страны проживания¹². Очевидно, указанные положения о применимом праве касаются отношений между пользователями и компанией Airbnb, но не затрагивают отношения между пользователями по поводу предоставления жилых помещений или оказываемых ими услуг. Как указано в Условиях, хозяева несут единоличную ответственность за изучение, понимание и соблюдение всех законов, правил и норм, применимых к их

объявлениям и услугам. Например, законодательство некоторых городов ограничивает возможность возмездного приема гостей на короткие сроки или предоставления определенных услуг хозяина. Во многих городах хозяевам нужно зарегистрироваться, получить разрешение или лицензию на предоставление определенных услуг (например, на приготовление пищи, продажу алкоголя, проведение экскурсий или вождение транспортных средств). Хозяева несут единоличную ответственность за сбор необходимой информации и получение всех лицензий, разрешений или регистраций, необходимых для предоставления услуг. Некоторые виды услуг хозяина могут быть запрещены под угрозой штрафов и иных мер воздействия¹³.

Таким образом, Airbnb, как и аналогичные сайты, представляет собой маркетплейс, который не владеет объектами недвижимости и не заключает договоры по поводу нее, а только оказывает услуги пользователям, обеспечивая возможность поиска наиболее удачных для пользователя предложений за плату. Договоры о пользовании недвижимым имуществом заключаются непосредственно между «хозяевами» и «гостями». Как указано выше, в Условиях предоставления услуг на сайте Airbnb такие договоры обозначены как договоры аренды. При этом в настоящее время сайт также предоставляет пользователям возможность размещать объявления об оказании ими услуг (экскурсии, впечатления, мероприятия и т.п.). В связи с этим договоры, заключаемые между пользователями, могут носить смешанный характер, включать в себя, помимо предоставления жилья, также сопутствующие услуги (приготовление еды, экскурсии, трансфер и т.п.). Важно, что и хозяева, и гости присоединяются к условиям предоставления услуг, размещенным на сайте Airbnb, в связи с чем, думается, нельзя рассматривать договоры, заключаемые между компанией и пользователями и между пользователями, в отрыве друг от друга, эти договоры образуют определенную систему, что вполне

¹¹ Airbnb. URL: <https://www.airbnb.ru/terms/> (дата обращения: 27.03.2019).

¹² Airbnb. URL: <https://www.airbnb.ru/terms#sec21> (дата обращения: 01.04.2019).

¹³ Airbnb. URL: <https://www.airbnb.ru/terms/> (дата обращения: 01.04.2019).

соответствует теории сетевого договора¹⁴, компания предоставляет хозяевам и гостям гарантии, связанные с причинением вреда имуществу, отменой резервирования и т.п.

Можно ли говорить о том, что данные договоры относятся к договорам по оказанию гостиничных услуг и не содержат элементы договора аренды или найма жилого помещения? В свете последних изменений ст. 17 Жилищного кодекса Российской Федерации (редакция вступит в силу с 01.10.2019)¹⁵, согласно которой запрещено размещать в жилых помещениях гостиницы, а жилое помещение в многоквартирном доме не может использоваться для предоставления гостиничных услуг, указанный вопрос приобретает особое значение.

Исходя из буквального толкования действующих норм, гостиничные услуги определяются как комплекс услуг по обеспечению временного проживания в гостинице, включая сопутствующие услуги, перечень которых определяется исполнителем¹⁶. Правила оказания гостиничных услуг не распространяются на деятельность молодежных туристских лагерей и туристских баз, кемпингов, детских лагерей, ведомственных общежитий, сдачи внаем для временного проживания меблированных комнат, а также деятельности по предоставлению мест для временного проживания в железнодорожных спальнях вагонов и прочих транспортных средствах. Гостиница, отель определяется как средство размещения, представляющее собой имущественный комплекс, включающий в себя здание или часть здания, помещения и иное имущество, в котором предоставляются услуги размещения и, как правило, услуги питания,

имеющее службу приема, а также оборудование для оказания дополнительных услуг; хостел рассматривается как вид гостиниц, включающих в себя многоместные номера, но не более 12 мест в одном номере, помещения для совместного использования гостями (гостиные, холлы, комнаты для завтраков и т.п.), общая суммарная площадь которых составляет не менее 25 % общей суммарной площади номеров, санитарные объекты, расположенные, как правило, за пределами номера, и предоставляющих услуги питания с ограниченным выбором блюд и (или) кухонное оборудование, а также по возможности дополнительные услуги¹⁷.

Таким образом, буквальное толкование нормативных правовых актов позволяет сделать вывод о том, что сдача внаем для временного проживания жилья напрямую не подпадает под определение гостиничных услуг, если не содержит всех их признаков, в связи с чем в настоящее время заключаемые по поводу жилых помещений соглашения могут содержать в себе элементы договоров, направленных на предоставление правомочия пользования (например, аренды или найма жилого помещения), а в некоторых случаях и договора оказания услуг, что позволяет говорить о том, что в рамках возникших отношений может быть заключен смешанный договор. В последнем случае, очевидно, услуги не должны являться центральным элементом заключаемого договора, поскольку возникает проблема разграничения с гостиничными услугами, оказание которых в жилых помещениях будет ограничено.

Можно ли говорить о том, что заключаемые договоры должны признаваться договорами

¹⁴ См. подробнее: *Кирпичев А. Е.* Неклассические теории договора (договор-обещание, дискретные, реляционные и сетевые договоры) в контексте новой редакции ГК России // *Законы России: опыт, анализ, практика.* 2016. № 2. С. 51—58; *Teubner G.* Networks as Connected Contracts. Oxford, 2011. P. 107, 213, 250; *Luhman N.* Law as a Social System. Oxford, 2008. Pp. 395—396.

¹⁵ Проект Федерального закона № 876688-6 «О внесении изменений в статью 17 Жилищного кодекса Российской Федерации» (ред. согласительной комиссии, принятая ГД ФС РФ от 04.04.2019) // СПС «КонсультантПлюс».

¹⁶ Постановление Правительства РФ от 09.10.2015 № 1085 (ред. от 30.11.2018) «Об утверждении Правил предоставления гостиничных услуг в Российской Федерации» // СЗ РФ. 2015. № 42. Ст. 5796.

¹⁷ Постановление Правительства РФ от 16.02.2019 № 158 «Об утверждении Положения о классификации гостиниц» // СЗ РФ. 2019. № 8. Ст. 786.

коммерческого найма жилого помещения в смысле гл. 35 Гражданского кодекса Российской Федерации¹⁸ (далее — ГК РФ)? По договору найма жилого помещения одна сторона — собственник жилого помещения или управомоченное им лицо (наймодатель) — обязуется предоставить другой стороне (нанимателю) жилое помещение за плату во владение и пользование для проживания в нем (п. 1 ст. 671 ГК РФ). При этом объектом договора найма жилого помещения может быть изолированное жилое помещение, пригодное для постоянного проживания (квартира, жилой дом, часть квартиры или жилого дома) (п. 1 ст. 673 ГК РФ).

Очевидно, идея хоумшеринга не привязана к предоставлению именно изолированного жилого помещения во временное владение и пользование для проживания в нем. Например, изначально, чтобы подзаработать на аренде своей квартиры, основатели компании Airbnb придумали пускать участников большой конференции разработчиков, которым не хватало мест в забитых до отказа гостиницах Сан-Франциско, на ночлег на надувных матрасах в свою квартиру (отсюда и название компании)¹⁹. По условиям, размещенным на сайте компании, услуги хозяев могут включать в себя сдачу в аренду мест для проживания или *иных помещений*, для их обозначения используется термин «жилье», а не «жилое помещение» (как известно, в отечественном законодательстве термин «жилое помещение» закреплен легально²⁰ и не совпадает с термином «жилище», «жилье» и т.п.). Например, «хозяева» предлагали дом на дереве, баржу, замок, индейский вигвам²¹. Таким образом, по своей конструкции заключаемые между «хозяевами» и «гостями» договоры по поводу пользования жильем могут признаваться как договорами аренды, так и (в некоторых случаях при обнаружении всех признаков и особенно-

стей) договорами коммерческого найма жилого помещения. Подобный сайт можно создать для предоставления жилых помещений на безвозмездных началах, тогда указанная конструкция подпадет под действие норм о договоре ссуды.

Однако анализ действующих положений гражданского законодательства о перечисленных выше типах договоров показывает, что не все нормы в их действующей редакции могут быть применены к отношениям краткосрочного пользования недвижимым имуществом в рамках экономики совместного потребления. Например, положения о преимущественном праве аренды, распределение прав и обязанностей сторон (в частности, обязанности по текущему ремонту или внесению коммунальных платежей), о судебном порядке расторжения договора аренды при существенном нарушении условий договора одной из сторон. Безусловно, большинство перечисленных норм являются диспозитивными, что дает сторонам возможность урегулировать возникшие отношения по краткосрочному пользованию недвижимым имуществом в договоре иным образом (главное, чтобы стороны пользовались такой возможностью), хотя в любом случае, думается, требуют уточнения действующие нормы о договоре аренды и найма жилого помещения в части регулирования отношений по краткосрочной аренде и краткосрочному найму жилого помещения.

Необходимо отметить, что идея хоумшеринга (идея делить жилище, кров) не является новой. Она давно и успешно развивается во всем мире. В настоящее время такие программы есть в 16 странах от Канады до Кореи, от Австрии до Австралии. Эти программы обычно позволяют одиноким пожилым домовладельцам найти молодых компаньонов, жильцов, которые бесплатно или за небольшую плату получают кров в обмен

¹⁸ Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ (ред. от 29.07.2018) (с изм. и доп., вступ. в силу с 30.12.2018) // СЗ РФ. 1996. № 5. Ст. 410.

¹⁹ Галлахер Л. Airbnb. Как три простых парня создали новую модель бизнеса [пер. с англ. Е. Деревянко]. М.: Эксмо, 2019. С. 27.

²⁰ См.: п. 2 ст. 15 Жилищного кодекса Российской Федерации от 29.12.2004 № 188-ФЗ (ред. от 22.01.2019) // СЗ РФ. 2005. № 1 (ч. 1). Ст. 14.

²¹ Галлахер Л. Указ. соч. С. 13.

на оказываемую домовладельцу помощь, что позволяет решить множество социальных проблем, наладить связь между двумя поколениями²². Эти идеи перекликаются с самой сутью экономики совместного потребления, однако нужно ли исключать из понятия хоумшеринга возможность предоставления свободного жилья в целях извлечения дохода, прибыли? Очевидно, грань между обычными предпринимательскими отношениями и отношениями экономики совместного потребления в настоящее время размыта, однако мы не должны исключать указанные модели, которые в любом случае связаны с идеей шеринга, идеей «поделиться» предоставляемыми мощностями, неважно, можно ли получить в связи с этим доход или нет. Таким образом, не только отношения по безвозмездному предоставлению свободных жилых помещений в пользование должны быть отнесены к шерингу в чистом виде, но и предоставление жилых помещений за плату (важно помнить, что понятие арендной платы в ГК РФ очень широко, арендная плата не привязывается только к получению денежных сумм, но также выражается в получении иных благ, услуг и т.п., что в полной мере отражает идеи экономики совместного потребления). В тех же случаях, когда недвижимое имущество предоставляется с единственной целью систематического извлечения прибыли без всякой социально значимой цели, можно предположить, что указанная деятельность при наличии всех предусмотренных законом признаков может признаваться предпринимательской, в этом случае, очевидно, такая деятельность будет выходить за рамки экономики совместного потребления.

В настоящее время важным является определение того, относятся ли маркетплейсы, опосредующие отношения между владельцами недвижимости и лицами, желающими воспользоваться ею на время, к агрегаторам товаров (услуг) в смысле действующего законодательства о защите прав потребителей? В соответствии

с Законом РФ от 07.02.1992 № 2300-1 (ред. от 29.07.2018) «О защите прав потребителей»²³ (далее — Закон о защите прав потребителей) владелец агрегатора информации о товарах (услугах) — организация независимо от организационно-правовой формы либо индивидуальный предприниматель, которые являются владельцами программы для электронных вычислительных машин и (или) владельцами сайта и (или) страницы сайта в информационно-телекоммуникационной сети «Интернет» и которые предоставляют потребителю в отношении определенного товара (услуги) возможность одновременно ознакомиться с предложением продавца (исполнителя) о заключении договора купли-продажи товара (договора возмездного оказания услуг), заключить с продавцом (исполнителем) договор купли-продажи (договор возмездного оказания услуг), а также произвести предварительную оплату указанного товара (услуги) путем перевода денежных средств владельцу агрегатора в рамках применяемых форм безналичных расчетов в соответствии с п. 3 ст. 16.1 Закона о защите прав потребителей и Федеральным законом от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»²⁴.

Специфика предоставления в пользование недвижимого имущества, в частности жилых помещений, в большинстве случаев исключает возможность признания заключаемых между пользователями договоров потребительскими, поскольку чаще всего в таких случаях обе стороны договора либо не являются предпринимателями, либо, наоборот, приобретают право пользования недвижимостью не для личных целей (например, в случае с коворкингами), указанные договоры нельзя отнести к публичным договорам, поскольку их заключение основано на взаимном доверии сторон (важной частью большинства указанных сервисов является наличие возможности оставить отзыв о хозяине или госте). В связи с этим применение норм законодательства о защите прав потребителей не

²² См., например: Home Share international. URL: <https://homeshare.org/> (дата обращения: 01.04.2019); Homeshare. URL: <https://www.homeshare.com/> (дата обращения: 01.04.2019).

²³ СЗ РФ. 1996. № 3. Ст. 140.

²⁴ СЗ РФ. 2011. № 27. Ст. 3872.

выглядит вполне обоснованным в сфере аренды недвижимого имущества.

Однако в том случае, если речь идет о предоставлении возможности заключения договоров с профессиональными исполнителями-предпринимателями, оказывающими услуги по размещению граждан в целях систематического извлечения прибыли (например, гостиничные услуги), исключение возможности применения положений законодательства о защите прав потребителей не выглядит обоснованным, в связи с чем в этом случае, при наличии всех предусмотренных в законе о защите прав потребителей условий, к указанным отношениям могли бы применяться его нормы и соответствующий маркетплейс может быть признан владельцем агрегатора и нести ответственность по закону о защите прав потребителей.

Таким образом, складывающиеся между домовладельцем и пользователем отношения в сфере совместного использования недвижимого имущества при заключении договоров через маркетплейс могут быть опосредованы классическими договорными конструкциями (договором аренды, коммерческого найма жилого помещения, договором ссуды) или носить смешанный характер (как правило, с договором оказания услуг). В настоящее время вряд ли можно говорить о выделении в этой сфере самостоятельного договорного типа, тем не менее следует признать необходимость дальнейшего совершенствования и трансформации положений действующего законодательства в части регулирования отношений по краткосрочному пользованию недвижимым имуществом, поскольку не все положения закона отражают существо возникающих отношений в условиях развития экономики совместного потребления.

Нельзя забывать о существовании модели отношений экономики совместного потребления, в рамках которой совместное использование недвижимого имущества осуществляется несколькими домовладельцами. Думается, в действующем российском законодательстве такой модели отношений уделяется крайне мало внимания. Например, жилищное законодательство предусматривает решение всех вопросов через конструкцию сообщества собственников многоквартирного дома. При этом большинство норм жилищного законодательства носят императивный характер и не позволяют внедрить диспозитивные договорные начала в складывающиеся отношения (регламентирован порядок принятия решения собраний, возможные формы управления многоквартирным домом, все еще традиционно велика роль органов местного самоуправления в рассматриваемых отношениях и т.п.), что в какой-то мере сдерживает возможность развития частной инициативы и возможность настоящего объединения всех собственников и проживающих в жилых помещениях лиц.

В иных случаях (например, при возникновении права общей собственности) допускается возможность определения вопросов о порядке владения, пользования и распоряжения имуществом на основании соглашения между всеми собственниками (ст. 246, 247 ГК РФ), однако вопросы о содержании, правах и об обязанностях сторон при заключении указанных соглашений, о соотношении с абсолютным правом каждого собственника на имущество нельзя назвать однозначно решенными в отечественном праве. В связи с вышеуказанным, думается, эта сфера нуждается в дальнейшем развитии и реформировании.

БИБЛИОГРАФИЯ

1. *Бидуэлл Дж.* Это прорыв. 100 уроков бизнес-инноваций. — М. : Альпина Паблишер, 2019. — 264 с.
2. *Галлахер Л.* Airbnb. Как три простых парня создали новую модель бизнеса / пер. с англ. Е. Дервянко. — М. : Эксмо, 2019. — 384 с.
3. *Головецкий Н. Я., Гребенюк В. В.* Фундаментальные основы экономики совместного потребления // Вестник Московского университета имени С. Ю. Витте. Серия 1 : Экономика и управление. — 2017. — № 4. — С. 21—26.

4. *Кирпичев А. Е.* Неклассические теории договора (договор-обещание, дискретные, реляционные и сетевые договоры) в контексте новой редакции ГК России // *Законы России: опыт, анализ, практика.* — 2016. — № 2. — С. 51—58.
5. *Botsman R., Rogers R.* What's Mine Is Yours: The Rise of Collaborative Consumption // *HarperBusiness*, 2010. — 279 с.
6. *Orsi J.* Practicing law in the sharing economy: helping people build cooperatives, social enterprise, and local sustainable economies // *Cooperative societies — Law and legislation — United States. I. Title.* 2012. — 607 с.

Материал поступил в редакцию 6 мая 2019 г.

PECULIARITIES OF CIVIL LAW REGULATION OF RELATIONS CONCERNING GRANTING REAL ESTATE FOR USE IN THE CONTEXT OF DEVELOPMENT OF SHARED CONSUMPTION ECONOMY (SHARING ECONOMY)²⁵

AYUSHEEVA Irina Zoriktuevna, PhD in Law, Associate Professor of the Department of Civil Law of the Kutafin Moscow State Law University (MSAL)
aiusheeva@gmail.com
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

Abstract. *Currently, relations in the digital economy are developing in the context of the Fourth Industrial Revolution, and their regulation is changing. At the same time, environmental problems and limited resources are gradually changing attitudes towards the culture of consumption: there is a tendency to shift from the consumption society to the sharing economy characterized by the collective use of goods and services. These trends are evident in various areas, including ownership and the use of immovable property, in particular dwellings. Currently there are various services, such as Airbnb, that give an opportunity to grant real estate for use and such a format as sharing office space (co-working) is developing. It is relevant to define the nature of contracts that arise between users and owners of services or directly between users to establish the rights and obligations of the parties, the extent of their responsibility, which requires a more detailed study of the problem.*

Keywords: *real estate, joint use of a dwelling, contract, lease, commercial lease, smart contract, economy of shared consumption, digital economy, non-defined contract, civil law responsibility.*

REFERENCES (TRANSLITERATION)

1. Biduell Dzh. Eto proryv. 100 urokov biznes-innovacij. — М. : Al'pina Pabliher, 2019. — 264 s.
2. Gallaher L. Airbnb. Kak tri prostyh parnya sozdali novuyu model' biznesa / per. s angl. E. Derevyanko. — М. : Eksmo, 2019. — 384 s.
3. Goloveckij N. Ya., Grebenyuk V. V. Fundamental'nye osnovy ekonomiki sovmestnogo potrebleniya // *Vestnik Moskovskogo universiteta imeni S. Yu. Vitte. Seriya 1 : Ekonomika i upravlenie.* — 2017. — № 4. — С. 21—26.
4. Kirpichev A. E. Neklassicheskie teorii dogovora (dogovor-obeshchaniye, diskretnyye, relyatsionnyye i setevyye dogovory) v kontekste novoy redakcii GK Rossii // *Zakony Rossii: opyt, analiz, praktika.* — 2016. — № 2. — С. 51—58.

²⁵ The study was carried out with the financial support of RFBR within the framework of the scientific project No. 18-29-16054 «Conceptual Foundations of Legal Regulation of Relations Regarding Collective Use of Goods and Services (sharing economy) in the context of the development of digital technologies.»

Трансформации требований к форме договоров с учетом развития цифровых технологий¹

Аннотация. В статье рассмотрены основные вопросы совершенствования российского гражданского законодательства о форме сделки, большая часть которых связана с принятием Федерального закона от 18 марта 2019 г. № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации». Принятие данных изменений было обусловлено реализацией федерального проекта «Нормативное регулирование цифровой среды» в рамках национальной программы «Цифровая экономика Российской Федерации». Автором отмечено сходство воспринятых российским законодателем подходов с положениями международных актов, в частности Типового закона ЮНСИТРАЛ об электронной торговле 1996 г. и Конвенции ООН «Об использовании электронных сообщений в международных договорах» 2005 г. Сделан вывод, что в результате трансформации требований к форме договоров предусмотрены 2 основные вариации письменной формы (один документ, подписанный сторонами, и обмен документами) и 2 базовые фикции такой формы (акцепт действует на письменную оферту и совершение сделки с помощью электронных либо иных технических средств).

Ключевые слова: договор, сделка, оферта, акцепт, форма сделки, письменная форма, электронная форма, электронное сообщение, фикция письменной формы, цифровые технологии, цифровая экономика.

DOI: 10.17803/1994-1471.2019.103.6.049-057

Как известно, развитие цифровых технологий — реальность настоящего времени и фактор, который необходимо учитывать при правоприменении и в законотворческом процессе. Обеспечение ускоренного внедрения цифровых технологий в экономике и социальной сфере является одной из национальных целей развития Российской Федерации на период до 2024 г. (п. 1 Указа Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стра-

тегических задачах развития Российской Федерации на период до 2024 года»² (далее — Указ Президента РФ № 204)).

В соответствии с данным Указом Правительством Российской Федерации совместно с органами государственной власти субъектов Российской Федерации должна быть решена задача по созданию системы правового регулирования цифровой экономики, основанного на гибком подходе в каждой сфере, а также по внедрению гражданско-

¹ Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16200 «Трансформация концептуальных основ договорного права в условиях развития цифровых технологий: смарт-контракты и иные новеллы договорного регулирования».

² СЗ РФ. 2018. № 20. Ст. 2817.

© Гринь О. С., 2019

* Гринь Олег Сергеевич, кандидат юридических наук, доцент кафедры гражданского права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)

osgrin@msal.ru

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

го оборота на базе цифровых технологий (абз. 1 пп. «б» п. 11 Указа Президента РФ № 204).

Соответствующие положения включены в состав национальной программы «Цифровая экономика Российской Федерации»³, в рамках которой предусмотрена реализация федерального проекта «Нормативное регулирование цифровой среды» (проект 4.1)⁴.

В указанном проекте, в частности, речь идет о необходимости принятия федерального закона, *предусматривающего «урегулирование статуса совершаемых в письменной (электронной) форме сделок»*, а также автоматизированных («самоисполняемых») договоров (п. 1.3) (к слову, в Программе, утвержденной 28 декабря 2018 г., был установлен срок реализации данного мероприятия — 31 декабря 2018 г.) и принятия федерального закона, предусматривающего уточнение понятия электронного документа, определение процедур хранения документов, в том числе электронных, использования и хранения электронного дубликата (электронного образа) документа (п. 1.4).

Классические цивилистические положения, в том числе о форме сделок, содержащиеся в Гражданском кодексе Российской Федерации, в таких условиях подлежали оценке с позиций новой технологической реальности и необходимости реализации указанных программных документов.

Как известно, исходя из положений закона, договор в письменной форме может быть заключен путем:

- 1) составления одного подписанного сторонами документа;
- 2) путем обмена письмами, телеграммами, телексами, телефаксами и иными документами, в том числе электронными документами, передаваемыми по каналам связи, позволяющими достоверно установить, что документ

исходит от стороны по договору (п. 2 ст. 434 ГК РФ).

Общая фикция письменной формы закреплена в положениях п. 3 ст. 434 ГК РФ: она считается соблюденной, если письменное предложение заключить договор принято путем совершения лицом, получившим оферту, в срок, установленный для ее акцепта, действий по выполнению указанных в ней условий договора (отгрузка товаров, предоставление услуг, выполнение работ, уплата соответствующей суммы и т.п.), если иное не предусмотрено законом, иными правовыми актами или не указано в оферте (п. 3 ст. 438 ГК РФ).

Помимо этого, действующему гражданскому законодательству известны «упрощенные порядки» заключения договора.

В качестве примера можно привести лицензии в отношении программ для ЭВМ и баз данных (называемые в литературе «оберточными» лицензиями). Условия таких лицензионных договоров могут быть изложены на приобретаемом экземпляре программы для ЭВМ или базы данных либо на упаковке такого экземпляра, а также в электронном виде (п. 2 ст. 434 ГК РФ). Начало использования программы для ЭВМ или базы данных пользователем, как оно определяется указанными условиями, означает его согласие на заключение договора. В этом случае письменная форма договора считается соблюденной (п. 5 ст. 1286 ГК РФ).

Помимо этого, через категорию упрощенного порядка раскрывается понятие открытой лицензии на использование объектов авторских прав. Все условия такой лицензии должны быть доступны неопределенному кругу лиц и размещены таким образом, чтобы лицензиат ознакомился с ними перед началом использования соответствующего произведения. В открытой лицензии может содержаться указание на дей-

³ См.: Правовое регулирование экономических отношений в современных условиях развития цифровой экономики : монография / отв. ред. В. А. Вайпан, М. А. Егорова. М. : Юстицинформ, 2019 ; *Вайпан В. А. Правовое регулирование цифровой экономики // Предпринимательское право. Приложение «Право и бизнес». 2018. № 1. С. 12—17.*

⁴ Паспорт национальной программы «Цифровая экономика Российской Федерации», утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам (протокол от 24 декабря 2018 г. № 16) // URL: <http://government.ru/info/35568/> (дата обращения: 25.04.2019).

ствия, совершение которых будет считаться акцептом ее условий (ст. 438 ГК РФ). В этом случае письменная форма договора считается соблюденной (абз. 2. п. 1 ст. 1286.1 ГК РФ).

Указанные примеры «упрощенных порядков» заключения договоров — частные случаи фикции письменной формы, закрепленной в п. 3 ст. 434 ГК РФ.

Фактическая трансформация требований к форме сделок обусловлена тем известным обстоятельством, что на практике многие договоры достаточно давно заключаются с использованием сети «Интернет».

Можно выделить следующие разновидности таких способов заключения договоров: через интернет-сайты, посредством электронной почты.

Заключение договора посредством электронной почты отвечает предусмотренному в законе механизму «обмена документами» как одному из способов заключения договора в письменной форме (при использовании необходимых способов легализации соответствующей переписки).

В отношении заключения договора через интернет-сайты ситуация иная. Здесь используются две основные вариации заключения соглашений через интернет-сайты: *click-wrap* — пользователю предоставляется возможность ознакомиться с условиями договора и в случае согласия нажать соответствующую кнопку; *browse-wrap (web-wrap)* — при данной модели либо пользователю предоставляется возможность перейти по гиперссылке и при желании ознакомиться с условиями, либо высвечивается надпись о том, что, продолжая пользоваться этим сайтом, он принимает условия соглашения. При этом пользователь не выражает согласия с условиями в явной форме⁵.

Местом заключения договора, который оформлен с использованием Интернета, считается место жительства или нахождения лица, направившего предложение о заключении договора (оферту), если в договоре не указано иное (ст. 444 ГК РФ).

В научной литературе высказывались разные мнения в отношении соответствия *click-wrap*-соглашений требованиям о письменной форме сделки.

Так, например, В. С. Витко считает, что такого соответствия нет. Автор обосновывает свою позицию действовавшей на тот момент редакцией п. 3 ст. 1286 ГК РФ, в которой указывалось на возможность изложения условий договора на экземпляре программы для ЭВМ (в настоящее время — п. 5 указанной статьи). При этом, по его мнению, «соглашение заключается не в порядке, предусмотренном п. 3 ст. 438 ГК РФ, так как в этом случае отсутствует письменное предложение правообладателя заключить лицензионный договор и поэтому такие соглашения должны считаться недействительными (ничтожными) по причине несоблюдения письменной формы»⁶.

В свою очередь, А. И. Савельев полагает, что такое соответствие есть. В качестве аргумента автором приводятся положения п. 3 ст. 434 и п. 3 ст. 438 ГК РФ: «При заключении *click-wrap*-соглашения имеет место предложение заключить договор, исходящее от правообладателя (провайдера). Данное предложение изложено в письменной форме, т.е. с использованием алфавита, набора букв и иных письменных символов. Такое предложение можно расценивать как оферту, поскольку оно, как правило, содержит указания на его юридически обязывающий характер и намерение оферента считать себя связанным им в случае его акцепта пользователем... Поскольку в тексте соглашения имеются указания на то, что, кликая по кнопке «я согласен», пользователь выражает свое согласие с условиями договора, совершение таких действий является действием по выполнению указанных в оферте условий, т.е. акцептом письменной оферты конклюдентными действиями»⁷.

Как видно, спор здесь сводится к вопросу о квалификации соответствующих действий правообладателя, или потенциального продав-

⁵ См.: Савельев А. И. Электронная коммерция в России и за рубежом: правовое регулирование. М.: Статут, 2016. 640 с.

⁶ Витко В. С. Гражданско-правовая природа лицензионного договора. М.: Статут, 2011. 301 с.

⁷ Савельев А. И. Указ. соч.

ца, исполнителя, подрядчика и др. именно как письменной оферты.

По этому вопросу необходимо отметить, что наличие письменной оферты в случае заключения click-wrap-соглашений не подлежит оспариванию, когда такое предложение отвечает признакам, содержащимся в ст. 435 ГК РФ:

- достаточная определенность;
- выражение оферентом намерения считать себя заключившим договор с адресатом, которым будет принято предложение;
- содержание в тексте существенных условий договора.

Поэтому в большинстве случаев такие контракты могут быть квалифицированы как заключенные в письменной форме на основании п. 3 ст. 434 и п. 3 ст. 438 ГК РФ.

При совершении соглашений по модели browse-wrap (web-wrap) ситуация осложняется тем, что пользователь не выражает согласия с предлагаемыми условиями в явной форме⁸. Во многом это зависит от способа визуализации соответствующей информации на сайте, поэтому действия пользователя не всегда могут быть расценены как акцепт. В таких условиях вряд ли следует говорить о возможности определения общего правила о соответствии или несоответствии таких соглашений требованиям о письменной форме сделки. Поэтому решение этого вопроса возможно лишь в каждом конкретном случае с учетом фактических обстоятельств дела.

В приведенном выше положении национальной программы «Цифровая экономика Российской Федерации» речь идет об «урегулировании статуса совершаемых в письменной (электронной) форме сделок». Такая формулировка порождает вопросы не столько о правовом режиме соответствующих сделок, сколько о соотношении данных категорий — письменной формы и «электронной формы» сделок. Является ли такая форма самостоятельной или же исключительно разновидностью письменной формы? И если разновидностью, то в рамках

автономного способа наряду с уже известными ст. 160 ГК РФ и ст. 434 ГК РФ либо новой разновидностью реализации фикции письменной формы, предусмотренной п. 3 ст. 434 ГК РФ?

При регулировании данных отношений и решении этого вопроса важно учитывать международный и зарубежный опыт, в частности отраженный в документах унификации частного права.

Прежде всего необходимо отметить положения Типового закона ЮНСИТРАЛ об электронной торговле 1996 г.⁹ (далее — Типовой закон ЮНСИТРАЛ), где используется термин «сообщение данных» (data message), который раскрывается как информация, подготовленная, отправленная, полученная или хранимая с помощью электронных, оптических или аналогичных средств, включая электронный обмен данными (ЭДИ), электронную почту, телеграмму, телекс или телефакс, но не ограничиваясь ими.

В соответствии со ст. 11 Типового закона ЮНСИТРАЛ в контексте заключения контрактов, если стороны не договорились об ином, оферта и акцепт оферты могут производиться с помощью сообщений данных. В случае когда при заключении контракта используется сообщение данных, этот контракт не может быть лишен действительности или исковой силы на том лишь основании, что для этой цели использовалось сообщение данных.

В отношении письменной формы в Типовом законе ЮНСИТРАЛ зафиксировано правило о том, что когда законодательство требует, чтобы информация была представлена в письменной форме, это требование считается выполненным путем представления сообщения данных, если содержащаяся в нем информация является доступной для ее последующего использования (ст. 6).

Указанные положения нашли свое отражение в **Конвенции ООН «Об использовании электронных сообщений в международных договорах»** (принята резолюцией 60/21 Генеральной Ассамблеи от 23 ноября 2005 г.)¹⁰ (да-

⁸ См.: Савельев А. И. Указ. соч.

⁹ URL: http://www.uncitral.org/pdf/russian/texts/electcom/05-89452_Ebook.pdf (дата обращения: 25.04.2019)

¹⁰ URL: http://www.un.org/ru/documents/decl_conv/conventions/elect_com.shtml (дата обращения: 25.04.2019).

лее — Конвенция ООН). Так, в силу ст. 8 Конвенции ООН сообщение или договор не могут быть лишены действительности или исковой силы на том лишь основании, что они составлены в форме электронного сообщения (electronic communications); ничто в Конвенции ООН не требует от какой-либо стороны использовать или принимать электронные сообщения, однако ее согласие на это может быть выведено из поведений этой стороны.

Из статьи 9 Конвенции ООН следует вывод о том, что сделки, совершаемые посредством электронных сообщений, квалифицируются как *разновидность письменной формы сделок*: в случаях, когда законодательство требует, чтобы сообщение или договор были представлены в письменной форме либо предусматривает наступление определенных последствий в случае отсутствия письменной формы, это требование считается выполненным путем представления электронного сообщения, если содержащаяся в нем информация является доступной для последующего использования.

В Модельных правилах европейского частного права (Draft of Common Frame of Reference, DCFR) направление электронных сообщений или аналогичные этому конструкции в базовых нормах о формах сделок не упоминаются. В данном акте прежде всего раскрываются понятия электронной подписи, которое означает сведения, закрепленные в электронной форме, которые присоединены к другим сведениям или логически объединены с другими сведениями в электронной форме и которые используются как способ идентификации (I.-1:107(3)). При этом термин «электронный» означает относящийся к электронным, цифровым, магнитным, беспроводным, оптическим, электромагнитным или аналогичным техническим возможностям (I.-1:107(5)).

Вместе с тем в DCFR специально оговаривается (II.-9:103 (2)), что если *договор должен быть заключен с помощью электронных средств* (if a contract is to be concluded by electronic means), сторона, предложившая условия, которые не

были согласованы специально, может ссылаться на них в отношениях с другой стороной, только если они были доведены до другой стороны в форме текста.

Согласно данному акту заявление признается сделанным в письменной форме, если оно сделано в форме текста, состоящего из знаков, которые разборчиво изображены на бумаге или ином материальном носителе (1.-1:106).

В статье 1.-1:106 также раскрываются категории текстовой формы и материального носителя. Текстовая форма означает текст, который выражен с помощью букв алфавита или иных печатных знаков при помощи средств, позволяющих прочитать, записать и *воспроизвести на материальном носителе содержащуюся в тексте информацию*. Термин «материальный носитель» означает носитель, на котором информация может быть сохранена таким образом, чтобы *она была доступна для ознакомления в будущем* в течение достаточного, исходя из назначения информации, периода времени и чтобы ее было можно воспроизводить в неизменном виде¹¹.

Как следует из приведенных выше фрагментов международных актов, важнейшим критерием соответствия информации в электронной форме требованиям письменной формы является доступность и воспроизводимость информации для последующего использования.

При этом, исходя из формулировок, содержащихся в приведенных выше нормах Конвенции ООН и Типового закона ЮНСИТРАЛ, — «требование считается выполненным путем представления электронного сообщения (requirement is met by an electronic communication)» — можно говорить о закреплении в данных документах правила о фикции письменной формы сделки.

В то же время в законодательстве ряда иностранных государств используется понятие *электронной формы сделки*.

Так, например, в соответствии с § 126a (Elektronische Form) Германского гражданского уложения (ГГУ)¹² сделка, требующая письмен-

¹¹ Модельные правила европейского частного права = Draft of Common Frame of Reference : пер. с англ. / науч. ред. Н. Ю. Рассказова. М. : Статут, 2013.

¹² URL: <http://www.gesetze-im-internet.de/bgb/index.html> (дата обращения: 25.04.2019).

ной формы, может быть совершена в электронной форме и подписана квалифицированной электронной подписью. В § 312с ГГУ предусматривается возможность заключения договоров дистанционным способом.

В США модельные подходы находят свое отражение, в частности, в Едином образном законе США об электронных сделках 1999 г.¹³ Согласно данному закону стороны вправе согласовать использование *электронной формы (electronic form)*, электронной подписи, электронных средств безопасности и установить содержание сделки.

В законодательстве Сингапура, напротив, нашли отражение подходы, закрепленные в Типовом законе ЮНСИТРАЛ и Конвенции ООН. В Акте об электронных транзакциях 2010 г. (The Electronic Transactions Act, ETA)¹⁴ закрепляется понятие электронного документа или «электронной записи» (electronic record), а понятие электронной формы сделки не используется.

Решение вопроса о регламентации порядка совершения сделок с использованием цифровых технологий в нашей стране осуществлялось в рамках рассмотрения проекта федерального закона № 424632-7 «О внесении изменений в части первую, вторую и третью Гражданского кодекса Российской Федерации»¹⁵, который был внесен в Государственную Думу еще 26 марта 2018 г. В настоящее время соответствующий закон принят — Федеральный закон от 18 марта 2019 г. № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации»¹⁶ вступает в силу с 1 октября 2019 г.

Следует отметить, что данный законопроект существенно дорабатывался на разных стадиях его рассмотрения. В частности, в ходе доработки документа на этапе второго чтения был учтен ряд замечаний, отраженных в заключении Сове-

та при Президенте РФ по кодификации и совершенствованию гражданского законодательства от 17 января 2019 г.¹⁷

В результате положения п. 1 ст. 160 ГК РФ были дополнены абзацем 2, в котором указано, что письменная форма сделки считается соблюденной также в случае совершения лицом сделки *с помощью электронных либо иных технических средств, позволяющих воспроизвести на материальном носителе в неизменном виде содержание сделки*, при этом требование о наличии подписи считается выполненным, если использован любой способ, позволяющий достоверно определить лицо, выразившее волю. Законом, иными правовыми актами и соглашением сторон может быть предусмотрен специальный способ достоверного определения лица, выразившего волю.

Отрадно отметить, что в итоговом варианте закона нашла отражение формулировка, которая характеризует соответствующие технические средства как *позволяющие воспроизвести на материальном носителе в неизменном виде содержание сделки* — в первых вариантах документа такого положения не было, а именно оно имеет важнейшее значение для недопустимости нарушения прав участников оборота, в том числе потребителей. Такое решение полностью соответствует приведенным выше положениям международных документов (Конвенции ООН и Типового закона ЮНСИТРАЛ), где отражено требование воспроизводимости как условие для квалификации формы сделки как письменной.

Вместе с тем в итоговой версии Закона не учтено замечание, содержащееся в упомянутом выше заключении Совета по кодификации и совершенствованию гражданского законодательства о том, что не вполне понятно, что имеется в виду под «электронными либо иными аналогичными техническими средствами»

¹³ URL: <https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=dac19487-e89c-0305-53fd-b0da7d68d22f&forceDialog=0> (дата обращения: 25.04.2019).

¹⁴ Electronic Transactions Act — Singapore Statutes Online // URL: <https://sso.agc.gov.sg/Act/88> (дата обращения: 25.04.2019).

¹⁵ URL: <http://sozd.parliament.gov.ru/bill/424632-7> (дата обращения: 25.04.2019).

¹⁶ СЗ РФ. 2019. № 12. Ст. 1224.

¹⁷ URL: <http://privlaw.ru/povestka-36/> (дата обращения: 25.04.2019).

(в принятой редакции слово «аналогичными» отсутствует).

Очевидно, что оценка рисков неопределенности указанной формулировки после 1 октября 2019 г. будет предметом анализа правоприменительной практики.

В отношении установленного требования о наличии подписи («использован любой способ, позволяющий достоверно определить лицо, выразившее волю; законом, иными правовыми актами и соглашением сторон может быть предусмотрен специальный способ достоверного определения лица, выразившего волю») необходимо отметить, что системность такого решения, очевидно, будет завершена после совершенствования законодательства об идентификации. Такое совершенствование, по всей видимости, будет осуществлено на основе проекта федерального закона «О внесении изменений в отдельные законодательные акты (в части уточнения процедур идентификации и аутентификации)» (подготовлен Минкомсвязью России)¹⁸. Данным законопроектом предлагается дополнить положения Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» понятиями «идентификатор», «идентификация, аутентификация лица», ввести понятие и регулирование «цифрового профиля» (своего рода прообраза электронного паспорта), внести корреспондирующие изменения в Федеральные законы «О связи», «О персональных данных», «Об основах охраны здоровья граждан в Российской Федерации». Очевидно, что толкование положений ГК РФ о *любом способе, позволяющий достоверно определить лицо, выразившее волю*, будет корреспондировать с предлагаемыми изменениями законодательства об идентификации.

Изменениям также подвергся п. 2 ст. 434 ГК РФ, где новой редакции которого указано, что договор в письменной форме может быть заключен путем составления одного документа (в том числе электронного), подписанного сторонами, или обмена письмами, телеграм-

мами, электронными документами либо иными данными в соответствии с правилами абз. 2 п. 1 ст. 160 ГК РФ.

Помимо того что из прошлой системы описания обмена документами исключены не часто используемые на практике телексы и телефаксы (которые теперь, очевидно, могут отправляться в рамках использования «иных технических средств», о которых идет речь в новой редакции нормы п. 1 ст. 160 ГК РФ), гораздо более важен тот факт, что из ГК РФ исключается термин «электронный документ».

Согласно абз. 2 п. 2 ст. 434 ГК РФ (в ред. Федерального закона от 8 марта 2015 г. № 42-ФЗ), который утратит силу с 1 октября 2019 г., электронным документом, передаваемым по каналам связи, признается информация, подготовленная, отправленная, полученная или хранимая с помощью электронных, магнитных, оптических либо аналогичных средств, включая обмен информацией в электронной форме и электронную почту.

С 1 октября 2019 г. при толковании положений ГК РФ об электронных документах, которых, к слову, станет значительно больше (поскольку Федеральным законом от 18 марта 2019 г. № 34-ФЗ внесены изменения, касающиеся электронных документов, в нормы ст. 493 ГК РФ о розничной купле-продаже, ст. 860.2 ГК РФ о номинальном счете, ст. 940 ГК РФ о договоре страхования), необходимо будет руководствоваться положением, содержащимся в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Здесь под электронным документом понимается документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах (п. 11.1 ст. 2).

Как несложно заметить, законодатель отказался от предлагаемого ему изначально подхо-

¹⁸ Текст в соответствии с публикацией на сайте <http://regulation.gov.ru/> по состоянию на 25.03.2019 (по состоянию на 25 апреля 2019 г. не внесен в Государственную Думу).

да о выделении специальной категории «электронной формы сделки» (известного, в частности, германскому и американскому праву) и воспринял подходы, отраженные в Конвенции ООН и Типовом законе ЮНСИТРАЛ. Введен еще один случай фикции письменной формы договора, поскольку при совершении сделки с помощью электронных либо иных технических средств такая форма лишь «считается соблюденной».

Решение данного вопроса могло бы, в частности, осуществиться в рамках дополнения п. 3 ст. 438 ГК РФ нормой о том, что акцептом может считаться не только исполнение договора, но и совершение иных действий, указанных

в оферте (в том числе акцепта в электронном виде). Однако то решение, которое принял законодатель, в большей степени отвечает интересам стабильности таких сделок, поскольку снимает возможный аргумент о спорности природы оферты в электронной форме как письменной.

Таким образом, в результате состоявшихся изменений в положениях гражданского законодательства о письменной форме сделке предусмотрены 2 основные ее вариации (один документ, подписанный сторонами, и обмен документами) и 2 базовые фикции письменной формы (акцепт действием на письменную оферту и совершение сделки с помощью электронных либо иных технических средств).

БИБЛИОГРАФИЯ

1. Вайпан В. А. Правовое регулирование цифровой экономики // Предпринимательское право. Приложение «Право и Бизнес». — 2018. — № 1. — С. 12—17.
2. Витко В. С. Гражданско-правовая природа лицензионного договора. — М. : Статут, 2011. — 301 с.
3. Модельные правила европейского частного права = Draft of Common Frame of Reference : пер. с англ. / науч. ред. Н. Ю. Рассказова. — М. : Статут, 2013.
4. Правовое регулирование экономических отношений в современных условиях развития цифровой экономики : монография / отв. ред. В. А. Вайпан, М. А. Егорова. — М. : Юстицинформ, 2019. — 376 с.
5. Савельев А. И. Электронная коммерция в России и за рубежом: правовое регулирование. — М. : Статут, 2016. — 640 с.

Материал поступил в редакцию 6 мая 2019 г.

TRANSFORMATION OF CONTRACT FORM REQUIREMENTS BASED ON THE DEVELOPMENT OF DIGITAL TECHNOLOGIES¹⁹

GRIN Oleg Sergeevich, PhD in Law, Associate Professor of the Department of Civil Law of the Kutafin Moscow State Law University (MSAL)
osgrin@msal.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

Abstract. *The article deals with the main issues of improving the Russian civil laws concerning the form of transaction the majority of which are associated with the adoption of the Federal Law of March 18, 2019, No. 34-FZ «On Amendments to Parts I, II and Article 1124 of Part III of the Civil Code of the Russian Federation.» The adoption of amendments mentioned above was preconditioned by the implementation of the federal project «Normative*

¹⁹ The study was carried out with the financial support of RFBR within the framework of the scientific project No. 18-29-16081 «Transformation of the Conceptual Foundations of Contract Law in the Context of Digital Technologies Development: Smart Contracts and Other Novelties of Contract Regulation».

Regulation of the Digital Environment» within the framework of the National Program «Digital Economy of the Russian Federation.» The author highlights similarity of approaches perceived by the Russian law-maker with the provisions of international instruments, in particular the UNCITRAL Model Law on Electronic Commerce of 1996 and the UN Convention on «The Use of Electronic Communications in International Contracts» 2005. It is concluded that, as a result of transformation of requirements for the form of contracts, 2 main variations of written form (a single document signed by the parties, and exchange of documents) and 2 basic fictions of this form (accepting by conduct of a written offer and making a transaction by electronic or other technical means) have been approved.

Keywords: *contract, transaction, offer, acceptance, form of transaction, written form, electronic form, electronic communication, fiction of a written form, digital technologies, digital economy.*

REFERENCES (TRANSLITERATION)

1. *Vajpan V. A. Pravovoe regulirovanie cifrovoj ekonomiki // Predprinimatel'skoe pravo. Prilozhenie «Pravo i Biznes». — 2018. — № 1. — S. 12—17.*
2. *Vitko V. S. Grazhdansko-pravovaya priroda licenzionnogo dogovora. — M. : Statut, 2011. — 301 s.*
3. *Model'nye pravila evropejskogo chastnogo prava = Draft of Common Frame of Reference : per. s angl. / nauch. red. N. Yu. Rasskazova. — M. : Statut, 2013.*
4. *Pravovoe regulirovanie ekonomicheskikh otnoshenij v sovremennykh usloviyah razvitiya cifrovoj ekonomiki : monografiya / otv. red. V. A. Vajpan, M. A. Egorova. — M. : Yusticinform, 2019. — 376 s.*
5. *Savel'ev A. I. Elektronnaya kommerciya v Rossii i za rubezhom: pravovoe regulirovanie. — M. : Statut, 2016. — 640 s.*

ГРАЖДАНСКОЕ И АДМИНИСТРАТИВНОЕ СУДОПРОИЗВОДСТВО

И. И. Черных*

Правовое прогнозирование в сфере гражданского судопроизводства в условиях развития информационных технологий¹

***Аннотация.** Статья посвящена исследованию возможностей применения методик и средств юридического прогнозирования в сфере законотворчества, правоприменительной судебной деятельности и в сфере оказания юридической помощи в условиях развития информационных технологий применительно к гражданскому судопроизводству. На примере анализа одного из законопроектов в сфере гражданского судопроизводства тестируются технологии прогнозирования. Рассматриваются вопросы о формировании рабочих групп футурологов, о сборе информации при исследовании прогнозного фона при помощи цифровых технологий, о создании прогнозных правовых моделей при учете правовых рисков с использованием прикладных компьютерных программ. Подчеркивается значимость участия научной общественности в юридическом прогнозировании, а также необходимость разработки основ правового регулирования использования прогностических технологий и необходимость государственного контроля за этой деятельностью.*

***Ключевые слова:** юридический (правовой, предиктивный) прогноз, судебное правоприменение, законотворчество, прогностическая правовая ситуация, прогнозный фон, прогнозная модель, правовой мониторинг, информационные технологии, искусственный интеллект, процессуальные риски.*

DOI: 10.17803/1994-1471.2019.103.6.058-072

Применительно к одной из позиций мышления, заключающейся в том, что «сегодня» — это лишь неощутимый промежуток между «вчера» и «завтра», можно говорить, что степень точности предвосхищения будущего

зависит лишь от качественного и количественного уровня анализа уже случившегося. С другой стороны, будущее определяется не только представлением о том, каким оно могло бы быть (особенно если речь идет об узкоспеци-

¹ В рамках исполнения гранта РФФИ 18-29-16060 за 2018 год «Влияние цифровых технологий на гражданское и административное судопроизводство». Статья написана с использованием СПС «КонсультантПлюс».

© Черных И. И., 2019

* Черных Ирина Ильинична, кандидат юридических наук, доцент кафедры гражданского процесса Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
ch6363@yandex.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

альных знаниях в отдельных сферах бытия), но и направлением воли многих субъектов на достижение социально приемлемых результатов человеческого развития. С этой точки зрения глобальная футурология не является механической суммой разрозненных прогностических данных, но и существовать в их отсутствие она тоже не может. Следовательно, надо отталкиваться в методологии прогностических исследований от неизбежности диалектического взаимовлияния глобальных и специальных аналитических исследований. Правовое прогнозирование является важнейшей частью социального прогнозирования, в свою очередь, актуальность прогнозирования, сфокусированного на процессуальной стороне права, нельзя переоценить, поскольку оно прямо относится к области урегулирования конфликтов, т.е. имеет остросоциальную направленность.

В нашей стране начало исследованиям юридического прогнозирования положено в 70-е гг. прошлого столетия². Этим вопросам посвящены работы таких правоведов, как В. И. Никитинский, И. С. Самощенко, М. Д. Шаргородский, В. В. Глазырин, Т. Г. Морщакова, Е. А. Павлодский, О. А. Гаврилов, В. М. Сырых и др.³ Исследуется данная проблематика и на уровне диссертационных исследований⁴.

Однако многие серьезные научные разработки в этой сфере оказались не востребованными правовой практикой. И еще в 2006 г. в научной литературе отмечалось, что отсутствие теоретико-методологических принципов про-

гнозирования в отраслевых правовых науках приводит к тому, что процессы формирования перспективных направлений развития предмета и метода отрасли имеют в большей степени умозрительный, а не прогностический характер⁵. Можно предположить, что одной из объективных причин такого положения являются высочайшие требования к интеллектуальным усилиям и трудозатратам, необходимым для юридического прогнозирования в стадии практической реализации.

В настоящее время ситуация не слишком изменилась. Главные направления, остро нуждающиеся в развитии прогнозирования, — сфера законодательства и сфера его реализации, точнее правотворчество и правоприменение, а значит, нуждаются в нем и отраслевые юридические знания, обслуживающие данные области. В условиях развития цифровых технологий обработки информации потенциал юридического прогнозирования способен возрасти в больших масштабах. Характерно, что потребность в разработке обеих предметных сфер прогнозирования может быть показана на основе анализа деятельности судов, рассматривающих гражданские дела.

Следует воспользоваться разработками общей теории права в исследовании методологии юридического прогнозирования применительно к законотворчеству. Возможно выделение нескольких этапов прогнозирования, в ходе которых применяются соответствующие методики, средства и технологии. Это формулиро-

² См.: Егорова Н. Е., Иванюк О. А. Правовая реальность и юридическое прогнозирование // Журнал российского права. 2009. № 12. С. 152.

³ Например: Шаргородский М. Д. Прогноз и правовая наука // Правоведение. 1971. № 1; Глазырин В. В., Лапаева В. В., Морщакова Т. Г., Павлодский Е. А., Сырых В. М., Чеснокова М. Д., Яни С. А. Методология и методика прогнозирования эффективности действия правовых норм. М., 1986; Сырых В. М. Прогнозирование эффективности норм права на стадии их разработки // Труды ВНИИСЗ. Вып. 36. М., 1987; Глазырин В. В. Прогнозирование эффективности правовых норм: возможный подход // Труды ВНИИСЗ. Вып. 41. М., 1988; Павлодский Е. А. Опыт прогнозирования эффективности правового акта с помощью экспертных оценок // Труды ВНИИСЗ. Вып. 41. М., 1988; Гаврилов О. А. Стратегия правотворчества и социальное прогнозирование. М., 1993.

⁴ Например: Ломтева В. С. Прогнозирование в правотворчестве и правоприменении : автореф. дис. ... канд. юрид. наук. М., 2006; Погодина И. В. Проблемы планирования в российской юридической практике : автореф. дис. ... канд. юрид. наук. М., 2004.

⁵ Ломтева В. С. Указ. соч. С. 8.

вание прогностической проблемной ситуации, исследование прогностического фона, разработка прогностического сценария (прогностической модели).

I. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ПРОГНОЗИРОВАНИЯ В СФЕРЕ ГРАЖДАНСКОГО ПРОЦЕССУАЛЬНОГО ЗАКОНОДАТЕЛЬСТВА

Выберем в качестве объекта для тестирования технологий прогнозирования закон, который в широких юридических кругах получил образное название «процессуальная революция»⁶. Что представлял бы собой этот акт на стадии законопроекта, если его составители основывались бы на определенном прогностическом сценарии? Его формирование требует постановки соответствующих целей и задач.

В пояснительной записке к данному законопроекту указана цель, весьма, с нашей точки зрения, абстрактная — совершенствование процессуального законодательства. В качестве задач обозначаются унификация и оптимизация процедур и правил, применяемых при разрешении споров и иных юридических дел. Анализ текста законопроекта показывает максимальное стремление именно к оптимизации процесса, причем за счет «расширения применения принципа процессуальной экономии в том виде, в каком его понимают инициаторы изменений»⁷. Действительно, большинство предлагаемых изменений аргументировано необходимостью разгрузить суды. И в качестве желаемых последствий применения закона его разработчики спрогнозировали ускорение разрешения дел, увеличение степени доступности

судебной защиты, повышение эффективности защиты прав граждан и организаций, улучшение качества правосудия.

Демагогичность текста пояснительной записки с подобными формулировками с очевидностью демонстрируют декларативный, неконкретный и, следовательно, неопределенный характер целей данного реформирования, при слабо завуалированной направленности предлагаемых изменений на обустройство процесса к удобству судей, но не сторон.

Весьма полезен на данном этапе законопроектной работы был бы опыт использования информационных технологий для построения прогностического сценария с учетом так называемого прогностического фона.

В. Е. Новичков, исследуя возможности прогнозирования для нужд уголовно-политических предположений в сфере борьбы с преступностью, отмечает: формулирование прогностической проблемной ситуации, в сущности, отражает состояние социально-экономических факторов, явлений и процессов, устанавливает существенные изменения в поведении людей, их сознании, режима соблюдения уголовно-правовых и уголовно-политических предписаний⁸.

Как отмечается в литературе, реформе препятствует недостаточная действенность закона в самом государственном аппарате: традиционная непроработанность правовой иерархии, сохранение клиентских и патримониальных связей⁹. К институциональным проблемам судебной власти относят сверхцентрализацию судебной системы на федеральном уровне, политизацию российского правосудия и социально стратифицированное правосудие. Отмечаются

⁶ Постановление Пленума Верховного Суда РФ от 03.10.2017 № 30 «О внесении в Государственную Думу Федерального Собрания Российской Федерации проекта федерального закона «О внесении изменений в Гражданский процессуальный кодекс Российской Федерации, Арбитражный процессуальный кодекс Российской Федерации, Кодекс административного судопроизводства Российской Федерации и отдельные законодательные акты Российской Федерации»».

⁷ Халатов С. А. Процессуальная реформа: обсуждение предлагаемых новелл в процессуальное законодательство // Арбитражный и гражданский процесс. 2017. № 12. С. 40.

⁸ Новичков В. Е. Архитектура информационных ресурсов уголовно-политического прогнозирования: понятие, структура, объем // Таврический научный обозреватель. 2016. № 10 (15). С. 36.

⁹ Соломон-мл. П. Г. Судебная реформа в России // Отечественные записки: правосудие в России. 2003. № 2. С. 79.

также кадровые проблемы российского правосудия, отсутствие механизмов, обеспечивающих независимость судей. Отсутствие механизмов участия граждан в осуществлении правосудия акцентируется особенным образом. Уровень доверия граждан к суду неуклонно падает. А. А. Кондрашев приводит весьма убедительные данные об этом, основываясь на результатах социологических исследований¹⁰.

В юридическом обиходе давно поднята тема «пустых исков». В частности, прокуроры, очевидно имеющие годовой план по предъявлению исков в суды для реализации своей правозащитной функции, проявляют чудеса изобретательности в погоне за показателями.

Так, прокурор Засвияжского района города Ульяновска в интересах неопределенного круга лиц обратился в суд с иском к индивидуальному предпринимателю Ф. Г. Мухутдинову о признании действий по продаже алкогольной продукции с 23 часов до 8 часов по местному времени незаконными и об обязанности прекратить продажу алкогольной продукции с 23 часов до 8 часов по местному времени¹¹ (вместо более адекватных и оперативных мер прокурорского реагирования).

Пример показывает, что ресурсы для разгрузки судов не сосредоточены только лишь в изолированном совершенствовании процессуального законодательства. Многие специалисты видят проблему неразвитого в целом механизма системного правового мониторинга. Возможности информационных технологий способны суще-

ственно повысить объективность оценки существующего уровня правового регулирования и на следующем этапе проектировать модели правовых средств.

Не менее важна помощь искусственного интеллекта в получении и обработке информации, используемой для прогнозирования. Один из самых важных источников информации для последующей обработки в целях перспективного планирования — ресурсы, обеспечивающие обратную связь с участниками судопроизводства на сайтах судов. Речь идет о таких опциях, как «Внепроцессуальные обращения», «Сообщение о технической проблеме», «Противодействие коррупции» и т.п. Эти «электронные приемные» должны стать объектом постоянного мониторинга со стороны компетентных органов и учитываться при решении правоприменительных проблем.

Еще одним важным элементом при исследовании прогнозного фона, пользуясь терминологией маркетологов, можно назвать «анализ конкурентной среды». В контексте тематики юридического прогнозирования возможно обращение к мониторингу альтернативных юрисдикционных форм защиты прав¹².

В одном из исследований, посвященных, в частности, тенденциям развития альтернативного разрешения споров (АРС), всесторонне изучается возможность передачи правосудия как исключительно государственной функции частным лицам — идея приватизации правосудия. Именно с этими формами разрешения право-

¹⁰ В 2010 г. для решения проблем в суд предпочло бы обратиться 41 % россиян, а в 2013 г. — только 33 % по данным соцопросов, проведенных «Левада-центром» в 2010 и 2013 гг. (URL: <http://ruwest.ru/news/6728/>). Чуть меньшую цифру доверия судам дает ФОМ — 40 %, но следует учитывать, что в опросе было только два варианта ответа для респондентов: положительная или отрицательная оценка суда (см.: Доклад ФОМ «О судах и судьях» // URL: <http://fom.ru/Bezopasnost-ipravo/10551> (дата обращения: 02.04.2019)). При этом в 2015 г. впервые в рейтинге недоверия государственным институтам на первое место вышла судебная система: 24 % наших сограждан доверяют судам, а 49 % не доверяют (см.: Труды Института социологии РАН (ИС РАН) «Российское общество и вызовы времени» (2015 год) // URL: <http://tass.ru/obschestvo/1857915> (дата обращения: 28.08.2016)).

¹¹ Халатов С. Пустые иски // https://zakon.ru/blog/2018/04/24/pustye_iski (дата обращения: 09.04.2019).

¹² В России имеется нормативная основа для развития несудебных форм защиты права, в частности, принят Федеральный закон от 27.07.2010 № 193-ФЗ «Об альтернативной процедуре урегулирования споров с участием посредника (процедуре медиации)» (последняя редакция), Федеральный закон от 29.12.2015 № 382-ФЗ «Об арбитраже (третейском разбирательстве) в Российской Федерации» (последняя редакция).

вых конфликтов связаны надежды на решение таких проблем государственного правосудия, как загруженность судов, длительность рассмотрения гражданских дел, сложность порядка и дороговизна правосудия по гражданским делам. Е. Г. Стрельцова отмечает, что альтернативные варианты разрешения споров являются неизбежным выбором тех юрисдикций, где отказываются от принципа объективной истины¹³. Характеризуя промежуточные результаты развития «частного правосудия» в мировой юридической практике, автор отмечает, что АРС не обладают механизмами, способными гарантировать защиту интересов лиц, не участвовавших в АРС, и защиту публичных интересов. Любое решение, вынесенное в рамках частных процедур, лишено значения всеобщности; более того, информация о нем попросту недоступна для лиц, не участвовавших в споре¹⁴. Из этого следует, что при выстраивании прогнозного сценария необходимо учитывать: а) саму возможность обращения граждан и организаций к альтернативным вариантам урегулирования споров; б) плюсы и минусы государственной деятельности по осуществлению правосудия в сравнении с альтернативными юрисдикциями; в) состояние «рынка» АРС и перспективы его развития в кратко- и долгосрочной проекции.

Итак, использование самого общего инструментария из арсенала прогнозирования показывает, что постановка целей «процессуальной революции» вряд ли осуществлена в корреляции уровня общественного развития с измерениями его правового отражения.

Важным элементом прогнозирования является формирование рабочих групп. В зависимости от выполняемых задач и этапа составления прогнозного сценария, группы варьируются по качественному и количественному составу. Правовое прогнозирование требует

привлечения не только юристов, понимающих специфику правового регулирования отрасли. В группу футурологов должны войти представители иного общественно-отраслевого знания, способные учитывать социальные и экономические проблемы, связанные с предстоящими законодательными изменениями. Это политологи, экономисты, социологи, лингвисты и др. И конечно, специалисты в области информационных технологий, обладающие знаниями для обеспечения информационной структуры прогнозирования.

Нет никаких официальных сведений о составе группы разработчиков «процессуальной революции». Как правило, Управление систематизации законодательства и анализа судебной практики ВС РФ осуществляет подготовку законопроекта на основе обобщения правоприменительной практики, нередко организует опросы судей низших звеньев, руководствуется данными государственной статистической отчетности.

Как видно, «процессуальная революция» подготовлена внутри судейского сообщества. Но, как отмечают исследователи, «судебный» взгляд мало коррелирует с мнением наших сограждан, доверяющих судам даже меньше, чем иным государственным институтам. В группу разработчиков не были привлечены даже ученые из области гражданского судопроизводства. Пренебрежение методом экспертной оценки и методом выявления общественного мнения в сфере права привело к тому, что при первом же обнародовании законопроекта научная и бизнес-общественность резко критически выступила против большинства масштабных преобразований¹⁵.

Кратко остановимся на главных положениях критики в отношении правовых моделей, рассматриваемых ВС РФ в качестве наиболее

¹³ Стрельцова Е. Г. Приватизация правосудия. М., 2019. С. 34.

¹⁴ Стрельцова Е. Г. Указ. соч. С. 81.

¹⁵ Коллективное правовое заключение на законопроект ВС РФ о внесении изменений в ГПК РФ, АПК РФ, КАС РФ // URL: https://zakon.ru/blog/2017/12/17/kollektivnoe_pravovoe_zaklyuchenie_na_zakonoproekt_vs_rf_o_vnesenii_izmenenij_v_gpk_rf_apk_rf_kas_rf#_ftnref5; Верховный суд попросили скорректировать реформу процессуального законодательства // URL: <http://centrdelo.ru/verhovnyj-sud-poprosili-skorrektirovat-reformu-processualnogo-zakonodatelstva/> (дата обращения: 10.04.2019).

рациональных и призванных обеспечить динамичное развитие гражданского судопроизводства.

1. Развитие упрощенных форм судопроизводства.

Довольно успешный опыт применения норм об упрощенном производстве в арбитражных судах побудил инициаторов реформы бесспорные или «малозначительные» дела рассматривать в порядке упрощенного производства также и в судах общей юрисдикции. По преобладающему среди юристов мнению, норм об упрощенном производстве, содержащихся в АПК РФ и ГПК РФ, явно недостаточно для четкого и эффективного рассмотрения дел в таком порядке.

Приказное же производство большинством ученых не относится к порядку осуществления правосудия, поскольку в нем отсутствуют обеспечивающие его гарантии¹⁶.

2. Сокращение круга гражданских дел, по которым составляются мотивированные судебные решения.

Это предложение оценено профессиональным юридическим сообществом резко отрицательно¹⁷.

3. Расширение в судах института профессионального представительства.

На заседании Совета при Президенте РФ по правам человека, посвященном судебной реформе, председатель Совета судей России В. Момотов заявил, что запрет на непрофесси-

ональное представительство в суде — мировая тенденция, к которой движутся все развитые страны. «Представление интересов в суде не менее сложная задача, чем работа врача. Я допускаю, что некоторые люди без медицинского диплома могут оказать помощь не хуже профессионального медика. Но это не означает, что к врачам не должно предъявляться требование о наличии высшего образования или что такое требование нарушает чьи-то права», — объяснил В. Момотов. Это никак не похоже на содержательную аргументацию, более того, заявление свидетельствует об отсутствии общего представления о социальной структуре общества, отсутствии понимания, что на современном этапе дополнительная профессионализация гражданского судопроизводства способна затруднить доступ гражданам к правосудию и усугубить социальное расслоение.

Этот поверхностный обзор базовых положений «процессуальной революции», не прошедших утверждение законодателем, показывает, при какой информационной изоляции и аналитической недостаточности осуществляется законопроектная работа. Между тем весьма полезным оказалось бы применение информационных технологий не только для получения надежных исходных данных для анализа, но и для проверки достоверности результатов перспективного планирования правового регулирования, а также для выявления правовых рисков. В литературе считают необходимым

¹⁶ Следует отметить, что в юридической среде приказному производству как сокращенной и упрощенной модели защиты прав предлагается придать автоматизированную форму. Предлагается доверить эти дела программе с условным названием «ИИ-судья», которая будет выдавать судебный приказ полностью в автоматизированном режиме на основе использования цифровых технологий. См.: Барсегян А. Л. Автоматизированное приказное производство. Вторжение в правосудие или хорошая оптимизация? // URL: https://zakon.ru/blog/2018/2/14/avtomatizirovannoe_prikaznoe_proizvodstvo_vtorzhenie_v_pravosudie_ili_horoshaya_optimizaciya (дата обращения: 11.04.2019).

¹⁷ Без подведомственности и мотивировочной части. Верховный суд готовит масштабную реформу процесса // URL: https://zakon.ru/discussion/2017/09/26/bez_podvedomstvennosti_i_motivirovochnoj_chasti_verhovnyj_sud_gotovit_masshtabnyu_reformu_processa#comment_412815; Е. Борисова: «Снижение судебной нагрузки ставится во главу преобразований процессуального законодательства» // Гарант.ру. URL: <http://www.garant.ru/interview/1144157/#ixzz5hmtVwGip>; В Госдуме поспорили об отмене мотивировочной части судебных решений // URL: <https://legal.report/v-gosdume-posporili-ob-otmene-motivirovochnoj-chasti-sudebnyh-reshenij/> (дата обращения: 19.04.2019).

элементом правового прогноза выявление процессуальных рисков¹⁸. С его помощью возможно просчитать отклонения от предполагаемой цели, вероятность достижения желаемого результата и т.д.

С. В. Василькова предлагает управлять процессуальными рисками, убедившись прежде всего в том, что риск является реальным, а не теоретическим, и, что немаловажно в условиях цифровизации судопроизводства, оценка риска должна быть выражена через количественный или качественный показатели. Автор рассматривает такую технологию на примере конкретных рисков — связанных с электронным извещением в гражданском судопроизводстве¹⁹. Выявлены субъективные и объективные причины данных рисков. Так, выражая согласие на получение от суда извещений в электронном виде (на электронную почту, в виде СМС), лицо предположительно осознает, что оно должно осуществлять своевременную проверку электронной почты; использовать качественную технику; проявлять разумную осторожность в обращении с техникой и программным обеспечением во избежание поломки или иной неисправности, препятствующей получению электронного извещения. Можно считать это социальным договором в части принятия на себя обязанности использовать техническое устройство, принимающее сообщение, по назначению. Но вряд ли это можно признать юридической обязанностью, и следовательно, это субъективная основа процессуального риска.

Объективные причины процессуальных рисков в сфере электронного извещения связаны с сравнительной новизной институтов

электронного правосудия, с тем, что они только проходят свою апробацию в гражданском судопроизводстве. Например, среди объективных причин процессуальных рисков неизвещения участников дела называются: техническая неоснащенность судов, низкое качество сотовой связи и сети Интернет, а также форс-мажорные обстоятельства (поломка компьютера или потеря мобильного телефона). Из всего указанного следует, что риски от применения современных информационных технологий, по сути, возложены на стороны, которые оповещаются путем электронного извещения. В ходе юридического прогнозирования оценка процессуального риска способна привести к правильному законодательному решению. Технология юридического прогнозирования включают в себя множество методик и позволяет максимально сблизить эмпирическое и логическое в научных исследованиях, охватить и связать воедино не только методы прогнозирования, но и различные блоки, составляющие институциональное, функциональное и инструментальное в его природе и содержании²⁰.

Вместе с тем очевидно, что сегодня назрела необходимость директивного закрепления правил научного прогнозирования как при разработке перспективных планов развития законодательства, так и при разработке проектов конкретных нормативных правовых актов. В идеале любой значимый законопроект, вносимый в законодательный орган, должен сопровождаться не только финансово-экономическим обоснованием, но и материалами прогнозирования, проведенного по установленным нормативам независимыми исследователями²¹.

¹⁸ Решетникова И. В. Теория процессуального риска // Закон. 2012. № 6. С. 117—122 ; Юдин А. В. Категория «риск» в гражданском судопроизводстве // Вестник гражданского процесса. 2014. № 5. С. 11—53.

¹⁹ Василькова С. В. Доктринальный и практический аспекты применения категории «процессуальный риск» в сфере электронного правосудия // Вестник гражданского процесса. 2018. № 4. С. 87—95.

²⁰ Гатилова А. С. К вопросу о технологии правового прогнозирования // Вестник ОГУ. 2012. № 3 (139). С. 31—36.

²¹ Радченко В. И., Иванюк О. А., Плюгина И. В., Цирин А. М. Практические аспекты прогнозирования законодательства и эффективности применения прогнозируемых норм // Журнал российского права. 2008. № 8. С. 3—14.

II. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ПРОГНОЗИРОВАНИЯ В СФЕРЕ ПРАВОПРИМЕНЕНИЯ (ГРАЖДАНСКОГО СУДОПРОИЗВОДСТВА)

Судебное правоприменение позволяет выявить пробелы, противоречия и другие дефекты законодательства в процессе реализации правовых норм. Однако это не означает, что правовое прогнозирование малозначимо для правоприменительной деятельности. Например, В. С. Ломтева не просто изучает возможность применения техник прогнозирования в правоприменительном процессе, но и выявляет факторы, определяющие его эффективность. В их числе такие организационно-правовые и социально-психологические факторы, как социально-правовая актуальность и содержательная ценность нормы права; качество законодательной техники и юридической терминологии; профессиональные и морально-нравственные качества правоприменителя; степень информированности адресатов о содержании нормы права; уровень правосознания и правовой культуры населения и др.²²

Таким образом, техники прогнозирования уместны на любом этапе судебного правоприменения, в том числе и на первоначальном, при решении вопроса о возбуждении гражданского дела. Так, например, существуют различные подходы в судебной практике к решению вопроса о родовой подсудности дел о признании недействительным, о расторжении, об изменении условий брачного договора. Далеко не все суды считают, что поскольку порядок заключения, изменения и расторжения брачного договора урегулирован нормами семейного законодательства (при этом указанные дела не исключены из подсудности мировым судьям ст. 23 ГПК РФ), то их следует относить к иным спорам, возникающим из семейно-правовых отношений. Принятие решения по этому вопросу судьей на этапе возбуждения дела может быть обусловле-

но прогнозированием результатов возможного обжалования судебного определения с учетом позиций вышестоящих инстанций. Информационной основой прогноза здесь служит изучение практики по данной категории дел. Вместе с тем оценка социально-правовой актуальности нормы действительно значима на момент ее применения. В контекст прогнозного фона должна быть вовлечена любая информация об изменении социальной значимости нормативного установления. Так, например, Федеральный закон от 28.11.2018 № 451-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»²³ исключает практически все семейно-правовые споры из компетенции мирового судьи, за исключением дел о расторжении брака при отсутствии спора о детях и разделе имущества супругов при цене иска до 50 тыс. руб. Изменение отношения вышестоящей судебной инстанции к родовой подсудности споров, возникших из семейно-правовых соглашений, четко проявилось при разъяснении порядка применения судами законодательства при рассмотрении дел, связанных со взысканием алиментов, в постановлении Пленума Верховного Суда РФ от 26.12.2017 № 56²⁴. В пункте 1 данного постановления указано: «Районный суд рассматривает в качестве суда первой инстанции дела по искам об изменении, о расторжении или признании недействительным соглашения об уплате алиментов», — без обоснования, несмотря на вполне сложившуюся практику рассмотрения таких дел у мировых судей. Объяснением может служить иная, по сравнению с изначально подразумеваемой в законе, оценка социального эффекта от разрешения судом подобных споров.

В ходе судебного правоприменения целесообразно использовать технологии предиктивной (предсказательной) аналитики на основе технологий искусственного интеллекта в случаях, когда правовая ситуация носит вероятностный и поливариантный характер²⁵. Обеспечение до-

²² Ломтева В. С. Указ. соч. С. 12—15.

²³ Российская газета. № 272. 04.12.2018.

²⁴ Российская газета. № 297. 29.12.2017.

²⁵ Здесь речь не идет обо всех случаях, когда суду приходится оценивать процессуальное поведение в целях определения направленности волеизъявления на использование заинтересованными лицами

стоверности прогнозирования — одна из самых сложных задач. К числу факторов, снижающих ее уровень, можно отнести: ограниченность исходных данных, неадекватность представлений об объекте и предмете прогнозирования, наличие субъективной интерпретации данных и др. Даже при наличии соответствующего программного продукта ввод данных для аналитики — работа конкретного судьи, именно он должен определять направления анализа исходной познавательной ситуации, конкретизировать цели, задачи и границы прогнозирования и грамотно их интерпретировать.

Определенные инструменты, используемые при рассмотрении и разрешении гражданских дел, могут с относительной легкостью поддаваться алгоритмированию. Так, при оценке косвенных доказательств суд сопоставляет их с искомым по делу юридическим фактом, определяя характер их связи между собой. Учитывая, что она носит вероятностный характер, искусственный интеллект мог бы выявить связь каждого из собранных по делу косвенных доказательств, определяя количество совпадений о предполагаемой связи с юридически значимым обстоятельством, переводя вывод о его наличии или отсутствии на качественный уровень.

Наиболее сложны для типизации такие фрагменты производства по гражданскому делу (где тем не менее предиктивная аналитика особенно уместна), которые обусловлены осмыслением прогноза как важнейшей фазы поведенческого контроля. В частности, суд, исходя из предвидения относительно юридически значимого поведения участников дела, принимает решение относительно применения обеспечительных мер, обращения судебного акта к немедленному исполнению.

В этом направлении перспективно использование Big Data. Технология способна анализировать тысячи похожих дел по ключевым словам и выдавать свои прогнозы с учетом личности участника процесса. Это может быть взято за основу перспективного расчета судьей поведения участника в конкретном случае.

Для работы же суда с информацией, не лишенной субъективного элемента, больше подходит искусственная нейронная сеть (ИНС). ИНС самообучаема. Предиктивные возможности нейронной сети обусловлены ее способностью к обобщению и выявлению скрытых зависимостей между исходными данными. После обучения сеть способна предсказать будущее значение некой последовательности на основе изучения прогнозного фона: существовавших в прошлом или существующих в настоящий момент факторов. Проще говоря, на основании косвенных признаков ИНС понимает, что именно лицо собирается совершить. Это может упростить правоприменителю принятие решения относительно предполагаемого юридически значимого поведения субъекта.

Возможности Big Data и ряда сервисов²⁶, предлагающих поиск и обработку необходимой информации, способны существенно облегчить ее анализ. Но далеко не все разделяют мнение о безоговорочной пользе Big Data в праве: «Право абстрактно, ценностно-ориентировано, строит новое и строится на компромиссе. Big Data эмпирична, алгоритмична и детерминистична, не создает нового»²⁷. Авторы считают, этой технологии недостаточно объективности и не хватает теоретического базиса. Познание смысла подлежащего применению закона — крайне сложный творческий процесс, требующий глубоких теоретических и даже научных знаний.

своих процессуальных прав в соответствии с замыслом законодателя относительно целей правового регулирования. Фактическое предвидение судом результатов такого использования прав — предмет самостоятельного исследования.

²⁶ Наиболее популярные сервисы здесь: <https://www.relativity.com/>, <https://www.symantec.com/>, <https://www.exterro.com/e-discovery-software/> (дата обращения: 19.04.2019).

²⁷ См.: *Томаев И. О.* Big Data: возможности использования в юриспруденции // URL: https://zakon.ru/blog/2018/09/25/big_data_vozmozhnosti_ispolzovaniya_v_yurisprudencii#comment_475175 (дата обращения: 19.04.2019).

Поддержание теоретических знаний на должном уровне и их обновление считается обязанностью юриста. В правоприменительной практике же встречаются случаи, крайне сложные с точки зрения теории права. Это можно показать на примере применения аналогии закона. Арбитражный суд, решая при рассмотрении одного из дел вопрос о судебных расходах, высказал мнение о возможности применения по аналогии в арбитражном процессе ст. 99 ГПК РФ о присуждении компенсации за потерю времени. Арбитражным судом отмечено, что положения указанной статьи подлежат применению лишь в тех случаях, когда в судебном заседании будет доказано, что сторона недобросовестно заявила неосновательный иск. И только недоказанность неосновательности иска помешала арбитражному суду применить данную норму по аналогии.

Наличие теоретических знаний об аналогии процессуального права не позволило бы суду мотивировать отказ в ее применении таким образом. Отсутствие в АПК РФ нормы, сходной по содержанию со ст. 99 ГПК РФ, представляющей собой разновидность санкции, свидетельствует о том, что законодатель преднамеренно по-иному урегулировал отношения. Пробел в данном случае отсутствует²⁸.

Этим хотелось бы подчеркнуть важность обучения соответствующих программ всему богатству теоретических достижений правовой науки при создании технологий для аналитики и прогнозирования правовых решений. Эта информация также относится к области объективных источников и успешно может быть обработана для правоприменителя.

Изучение представленных на рынке программных продуктов, облегчающих аналитическую работу юриста, демонстрирует значительное превосходство частных компаний над правоприменителем, не имеющим в своем арсенале подобных сервисов. Например, российским юристам-судебникам доступен Legal

Research — программный продукт, позволяющий визуализировать найденную информацию по релевантным делам и статистике. Такой сервис мог бы стать неоценимым помощником при решении некоторых задач правосудия. Итак, ценность методик прогнозирования с использованием информационных технологий в судебной правоприменительной деятельности трудно переоценить.

Но следует обратить внимание также и на организационно-правовые эффекты прогнозирования в работе суда. Прикладные модули информационной системы способны обеспечить мониторинг загруженности конкретного суда, анализ структуры гражданских дел, анализ и прогнозирование социальной структуры субъектов гражданского процесса, в том числе половозрастного состава заявителей и другие показатели. Их учет значим для принятия управленческих решений, например о количественном составе судей в конкретном суде, о специализации судей в конкретном суде. Более того, методики прогнозирования позволяют предсказать периоды появления новых категорий дел, количественный подъем или спад обращений по отдельным видам споров. Так, развитие законодательства об ипотечном кредитовании и узаконенная возможность оплачивать ипотеку средствами материнского капитала, выплата которого осуществляется с 2007 г., предсказуемо привело к возникновению споров, связанных с распоряжением средствами материнского (семейного) капитала, в частности об определении доли родителей и детей в праве собственности на жилое помещение, приобретенное с использованием средств материнского (семейного) капитала, о разделе между супругами имущества, приобретенного с использованием средств материнского (семейного) капитала и др. Такой прогноз имеет значение, например, для организации курсов обучения, повышения квалификации судей по данным категориям дел.

²⁸ В литературе обосновано, что пробел в гражданском процессуальном праве существует, только когда не урегулированный правом определенный случай не просто имеет отношение к производству по делу, а объективно имеет существенное значение для процесса в целом или отдельной его стадии. См.: *Туманов Д. А. Пробелы в гражданском процессуальном праве*. М., 2008. С. 27.

III. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ПРОГНОЗИРОВАНИЯ, ПРИМЕНЯЕМЫЕ В СФЕРЕ ЧАСТНОЙ ЮРИДИЧЕСКОЙ ПРАКТИКИ

Самое большое распространение технологии прогнозирования нашли в сфере частной юридической практики.

В начале 10-х гг. нашего тысячелетия на страницах юридической печати заговорили о коллективном судебском разуме как функциональном инструменте. «Толкователем», или, иначе, предсказателем, судебных решений стала компьютерная программа, способная анализировать дело по 200 параметрам: кто был судьей, в чем суть иска, кто истец, кто ответчик, какие решения приняли низшие инстанции, какими нормами они руководствовались и т.п. Более того, программа самообучаема, может учитывать текущее состояние в регулировании общественных отношений. Программа, получившая в среде юристов название «электронно-рандомное правосудие», вызывала чаще негативные оценки²⁹.

Сегодня такой программный продукт в мире и на юридическом рынке России — обыденная реальность. Сама по себе деятельность по предсказанию исхода дела является в значительной части рутинной работой, но в значительной мере — аналитической, где логика как основной инструмент вполне освоена машинами, способными осуществлять такую работу на порядок глубже, детальнее и быстрее. Вот наиболее известные прикладные программы. При помощи технологии Case Strategy, за короткое время анализирующей множество релевантной информации, можно получить прогноз даже с учетом личности судьи, который будет рассматривать дело. E-discovery осуществляет поиск электронной информации путем обнаружения, сбора и представления сведений, хранящихся на цифровых носителях: в электронных письмах, презентациях, базах данных и любых других документах, способных быть доказательствами в судебном разбирательстве. Данная технология наиболее развита в США и Великобритании в силу прецедентной правовой системы.

В России созданы такие технологии, как Casebook — сервис для отслеживания и контроля судебных дел и компаний. Среди возможностей Casebook: автоматическая проверка компаний по 36 факторам риска; проверка связей на текущий момент и схемы аффилированности на любую дату; анализ бухгалтерской отчетности с акцентом на слабые места; арбитражная статистика и графики с исковой нагрузкой; данные по текущим и завершённым исполнительным производствам. Сервис «Контрагенты» по любой компании, у которой были суды, определяет индекс судебной активности. Индекс демонстрирует, как часто судится контрагент, затягивает ли он производство, активен ли в процессе, хорошо ли его юристы готовятся к заседаниям. Сервис покажет арбитражные дела компании и историю исполнительных производств, вычислит вероятность взыскания суммы сделки после суда. «Сутяжник» — автоматизированный сервис по подбору судебной практики, соответствующей содержанию текстовых документов, загружаемых в сервис пользователем (проекты исковых заявлений, отзывы на иски, претензии, уже принятые судебные решения или их проекты и другие документы), в которых излагается правовая проблема. «Правобот» подбирает практику двумя способами — по ключевому слову и фильтрам или по тексту иска, претензии, жалобы. Раскладывает найденные документы по инстанциям, судам и регионам. Детализирует от суда первой инстанции до высших судов. Находит похожие дела из миллионов. Алгоритм поиска учитывает: вид спора, обстоятельства, инстанцию, исход, участников судебного процесса.

Можно приводить и иные примеры использования информационных технологий для прогнозирования в сфере бизнес-услуг, а можно просто констатировать, что развитие информационных технологий и уровень вовлеченности искусственного интеллекта в коммерческой среде ошеломляет. Компьютерно-программные технологии, нейротехнологии, биотехнологии, технологии робототехники продолжают стремительно, очень интенсивно развиваться.

²⁹ Ирицян А. Толкователи судей: в США разработали программу, угадывающую 7 из 10 решений Верховного суда // URL: <http://pravo.ru/review/view/124329/?cl=A> (дата обращения: 18.04.2019).

Из всего этого нужно сделать несколько важных выводов.

А. В условиях информатизации использование технологий прогнозирования в сфере правовых отношений — необходимая ступень развития правового регулирования. Значимо, что оно вполне доступно для широкого использования в целях автоматизации процесса, для обеспечения поддержки принятия правовых решений как законодателем, так и правоприменителем.

Б. Необходим государственный контроль над прогнозированием в сфере законотворчества, правоприменения и при использовании в частной сфере юридических услуг (требуется разработка правовых основ, методологических основ, средств измерения достоверности юридического прогноза и т.д.), и определяющим должно стать участие представителей науки при решении задач по обеспечении такого контроля.

Аналитики выражают опасение, что столь быстрое развитие предиктивной аналитики связано не только с практическими нуждами, но и с использованием искусственного интеллекта для поведенческого управления и контроля.

Это весьма ярко показывает практика создания частных краудфандинговых платформ, таких как американский LexShares или российская Platforma, для привлечения инвестиций в судебные процессы, где потерпевший выступает против корпораций, что актуально в табачной, медицинской отраслях, в спорах с производителями товаров для населения. Это, по мнению

экспертов, может привести к усилению зависимости судей, присяжных и других участников судебного процесса от заранее сделанных прогнозов относительно итогов процесса, которые базируются не на каких-то предпочтениях и личных оценках, а исключительно на объективных статистических расчетах³⁰.

В. Частный бизнес является существенно более оснащенным средствами использования информационных технологий, чем государственные органы, в числе которых судебные. Суды в своей профессиональной деятельности применяют традиционное программное обеспечение и сервисы, связанные с документооборотом, и вообще не используют прогнозное программное обеспечение, базирующееся на искусственном интеллекте. Судебные органы, будучи лишеными возможностей, предоставляемых информационными технологиями, поставлены в заведомо проигрышную позицию по отношению к лицам, чьи правовые конфликты они разбирают.

И поскольку на современном этапе не представляется возможным обойтись без формирования информационно-прогностического пространства, государству следует обеспечивать суду возможность получать доступ к совокупности организационных, управленческих, правоприменительных информационных ресурсов, формируемых как самим государством, так и иными участниками информационных отношений.

БИБЛИОГРАФИЯ

1. Барсегян А. Л. Автоматизированное приказное производство. Вторжение в правосудие или хорошая оптимизация? // URL: https://zakon.ru/blog/2018/2/14/avtomatizirovannoe_prikaznoe_proizvodstvo_vtorzhenie_v_pravosudie_ili_horoshaya_optimizaciya.
2. Борисова Е. А. Снижение судебной нагрузки ставится во главу преобразований процессуального законодательства // Гарант.ру. URL: <http://www.garant.ru/interview/1144157/#ixzz5hmtVwGip>.
3. Василькова С. В. Доктринальный и практический аспекты применения категории «процессуальный риск» в сфере электронного правосудия // Вестник гражданского процесса. — 2018. — № 4. — С. 87—95.
4. Гаврилов О. А. Стратегия правотворчества и социальное прогнозирование. — М., 1993. — 128 с.

³⁰ Овчинский В., Бинецкий А. Судья с искусственным интеллектом // URL: http://zavtra.ru/blogs/sud_ya_s_iskusstvennim_intellektom (дата обращения: 19.04.2019).

5. *Гатилова А. С.* К вопросу о технологии правового прогнозирования // Вестник ОГУ. — 2012. — № 3 (139). — С. 31—36.
6. *Глазырин В. В., Лапаева В. В., Морщакова Т. Г., Павлодский Е. А., Сырых В. М., Чеснокова М. Д., Яни С. А.* Методология и методика прогнозирования эффективности действия правовых норм. — М., 1986. — С. 88—142.
7. *Глазырин В. В.* Прогнозирование эффективности правовых норм: возможный подход // Труды ВНИИСЗ. — Вып. 41. — М., 1988. — С. 23—33.
8. *Егорова Н. Е., Иванюк О. А.* Правовая реальность и юридическое прогнозирование // Журнал российского права. — 2009. — № 12. — С. 152—156.
9. *Ирицян А.* Толкователи судей: в США разработали программу, угадывающую 7 из 10 решений Верховного суда // URL: <http://pravo.ru/review/view/124329/?cl=A>.
10. *Ломтева В. С.* Прогнозирование в правотворчестве и правоприменении : автореф. дис. ... канд. юрид. наук. — М., 2006. — 23 с.
11. *Новичков В. Е.* Архитектура информационных ресурсов уголовно-политического прогнозирования: понятие, структура, объем // Таврический научный обозреватель. — 2016. — № 10 (15). — С. 83—92.
12. *Овчинский В., Бинецкий А.* Судья с искусственным интеллектом // URL: http://zavtra.ru/blogs/sud_ya_s_iskusstvennim_intellektom.
13. *Павлодский Е. А.* Опыт прогнозирования эффективности правового акта с помощью экспертных оценок // Труды ВНИИСЗ. — Вып. 41. — М., 1988. — С. 71—83.
14. *Погодина И. В.* Проблемы планирования в российской юридической практике : автореф. дис. ... канд. юрид. наук. — М., 2004. — 23 с.
15. Правовой мониторинг: актуальные проблемы теории и практики : монография / Д. Б. Горохов, В. И. Радченко, Н. Н. Черногор [и др.] ; под ред. Н. Н. Черногора. — М., 2010. — 232 с.
16. *Радченко В. И., Иванюк О. А., Плюгина И. В., Цирин А. М.* Практические аспекты прогнозирования законодательства и эффективности применения прогнозируемых норм // Журнал российского права. — 2008. — № 8. — С. 3—14.
17. *Решетникова И. В.* Теория процессуального риска // Закон. — 2012. — № 6. — С. 117—122.
18. *Соломон-мл. П. Г.* Судебная реформа в России // Отечественные записки: правосудие в России. — 2003. — № 2. — С. 79—86.
19. *Стрельцова Е. Г.* Приватизация правосудия. — М., 2019. — 271 с.
20. *Сырых В. М.* Прогнозирование эффективности норм права на стадии их разработки // Труды ВНИИСЗ. — Вып. 36. — М., 1987. — С. 17—28.
21. *Томаев И. О.* Big data: возможности использования в юриспруденции // URL: https://zakon.ru/blog/2018/09/25/big_data_vozmozhnosti_ispolzovaniya_v_yurisprudencii#comment_475175.
22. *Туманов Д. А.* Пробелы в гражданском процессуальном праве. — М., 2008. — 208 с.
23. *Халатов С.* Пустые иски // URL: https://zakon.ru/blog/2018/04/24/pustye_iski.
24. *Халатов С. А.* Процессуальная реформа: обсуждение предлагаемых новелл в процессуальное законодательство // Арбитражный и гражданский процесс. — 2017. — № 12.
25. *Шаргородский М. Д.* Прогноз и правовая наука // Правоведение. — 1971. — № 1. — С. 40—50.
26. *Юдин А. В.* Категория «риск» в гражданском судопроизводстве // Вестник гражданского процесса. — 2014. — № 5. — С. 11—53.

Материал поступил в редакцию 6 мая 2019 г.

LEGAL FORECASTING IN THE FIELD OF CIVIL PROCEEDINGS IN THE CONTEXT OF DEVELOPMENT OF INFORMATION TECHNOLOGIES³¹

CHERNYKH Irina Ilinichna, PhD in Law, Associate Professor of the Department of Civil Procedure of the Kutafin Moscow State Law University (MSAL)
ch6363@yandex.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

Abstract. *The article is devoted to the study of possibilities of application of methods and means of legal forecasting for law-making, judicial law-enforcement and rendering legal assistance in the context of the development of information technology in civil proceedings. Forecasting technologies are being examined on the example of the analysis of one of draft laws in the context of civil proceedings. The article deals with the issues of formation of working groups of futurologists, data collection during examination of the forecast background using digital technologies, creation of forecast legal models in assessing legal risks with the use of computer software applications. The author emphasizes the importance of participation of academic community in legal forecasting, as well as the need to develop the foundations of legal regulation of the use of prognostic technologies and the need for the State control in this area.*

Keywords: *juridical (legal, predictive) forecast, judicial enforcement, lawmaking, prognostic legal situation, forecast background, forecast model, legal monitoring, information technology, artificial intelligence, procedural risks.*

REFERENCES (TRANSLITERATION)

1. Barsegyan A. L. Avtomatizirovannoe prikaznoe proizvodstvo. Vtorzhenie v pravosudie ili horoshaya optimizaciya? // URL: https://zakon.ru/blog/2018/2/14/avtomatizirovannoe_prikaznoe_proizvodstvo_vtorzhenie_v_pравosudie_ili_horoshaya_optimizaciya.
2. Borisova E. A. Snizhenie sudebnoj nagruzki stavitsya vo glavu preobrazovaniy processual'nogo zakonodatel'stva // Garant.ru. URL: <http://www.garant.ru/interview/1144157/#ixzz5hmtVwGip>.
3. Vasil'kova S. V. Doktrinal'nyj i prakticheskij aspekty primeneniya kategorii «processual'nyj risk» v sfere elektronного pravosudiya // Vestnik grazhdanskogo processa. — 2018. — № 4. — S. 87—95.
4. Gavrillov O. A. Strategiya pravotvorchestva i social'noe prognozirovanie. — M., 1993. — 128 s.
5. Gatilova A. S. K voprosu o tekhnologii pravovogo prognozirovaniya // Vestnik OGU. — 2012. — № 3 (139). — S. 31—36.
6. Glazyrin V. V., Lapaeva V. V., Morshchakova T. G., Pavlodskij E. A., Syryh V. M., Chesnokova M. D., Yani S. A. Metodologiya i metodika prognozirovaniya effektivnosti dejstviya pravovyh norm. — M., 1986. — S. 88—142.
7. Glazyrin V. V. Prognozirovanie effektivnosti pravovyh norm: vozmozhnyj podhod // Trudy VNIISZ. — Vyp. 41. — M., 1988. — S. 23—33.
8. Egorova N. E., Ivanyuk O. A. Pravovaya real'nost' i yuridicheskoe prognozirovanie // Zhurnal rossijskogo prava. — 2009. — № 12. — S. 152—156.
9. Iricyan A. Tolkovateli sudej: v SShA razrabotali programmu, ugadyvayushchuyu 7 iz 10 reshenij Verhovnogo suda // URL: <http://pravo.ru/review/view/124329/?cl=A>.
10. Lomteva V. S. Prognozirovanie v pravotvorchestve i pravoprimenenii : avtoref. dis. ... kand. yurid. nauk. — M., 2006. — 23 s.

³¹ As part of implementation of the grant of RFBR 18-29-16060 for the year 2018 «The Influence of Digital Technologies on Civil and Administrative Proceedings.» The Article is written using the RLS «ConsultantPlus».

11. Novichkov V. E. Arhitektura informacionnyh resursov ugovovno-politicheskogo prognozirovaniya: ponyatie, struktura, ob»em // Tavricheskiy nauchnyj obozrevatel'. — 2016. — № 10 (15). — S. 83—92.
12. Ovchinskij V., Bineckij A. Sud'ya s iskusstvennym intellektom // URL: http://zavtra.ru/blogs/sud_ya_s_iskusstvennim_intellektom.
13. Pavlodskij E. A. Opyt prognozirovaniya effektivnosti pravovogo akta s pomoshch'yu ekspertnyh ocenok // Trudy VNIISZ. — Vyp. 41. — M., 1988. — S. 71—83.
14. Pogodina I. V. Problemy planirovaniya v rossijskoj yuridicheskoy praktike : avtoref. dis. ... kand. jurid. nauk. — M., 2004. — 23 s.
15. Pravovoj monitoring: aktual'nye problemy teorii i praktiki : monografiya / D. B. Gorohov, V. I. Radchenko, N. N. Chernogor [i dr.] ; pod red. N. N. Chernogora. — M., 2010. — 232 s.
16. Radchenko V. I., Ivanyuk O. A., Plyugina I. V., Cirin A. M. Prakticheskie aspekty prognozirovaniya zakonodatel'stva i effektivnosti primeneniya prognoziruemyh norm // Zhurnal rossijskogo prava. — 2008. — № 8. — S. 3—14.
17. Reshetnikova I. V. Teoriya processual'nogo riska // Zakon. — 2012. — № 6. — S. 117—122.
18. Solomon-mi. P. G. Sudebnaya reforma v Rossii // Otechestvennye zapiski: pravosudie v Rossii. — 2003. — № 2. — S. 79—86.
19. Strel'cova E. G. Privatizaciya pravosudiya. — M., 2019. — 271 s.
20. Syryh V. M. Prognozirovanie effektivnosti norm prava na stadii ih razrabotki // Trudy VNIISZ. — Vyp. 36. — M., 1987. — S. 17—28.
21. Tomaev I. O. Big data: vozmozhnosti ispol'zovaniya v yurisprudencii // URL: https://zakon.ru/blog/2018/09/25/big_data_vozmozhnosti_ispolzovaniya_v_yurisprudencii#comment_475175.
22. Tumanov D. A. Probely v grazhdanskom processual'nom prave. — M., 2008. — 208 s.
23. Halatov S. Pustye iski // URL: https://zakon.ru/blog/2018/04/24/pustye_iski.
24. Halatov S. A. Processual'naya reforma: obsuzhdenie predlagaemyh novell v processual'noe zakonodatel'stvo // Arbitrazhnyj i grazhdanskiy process. — 2017. — № 12.
25. Shargorodskij M. D. Prognoz i pravovaya nauka // Pravovedenie. — 1971. — № 1. — S. 40—50.
26. Yudin A. V. Kategoriya «risk» v grazhdanskom sudoproizvodstve // Vestnik grazhdanskogo processa. — 2014. — № 5. — S. 11—53.

ПРЕДПРИНИМАТЕЛЬСКОЕ И КОРПОРАТИВНОЕ ПРАВО

И. В. Ершова*,
Е. В. Трофимова**

Майнинг и предпринимательская деятельность: в поисках соотношения¹

***Аннотация.** В статье раскрыто содержание и намечены подходы к определению правовой природы майнинга. Обращено внимание на необходимость правового регулирования указанной деятельности, что предопределяется входящим в структуру национальной программы «Цифровая экономика Российской Федерации» федеральным проектом, предусматривающим нормативное регулирование цифровой среды. В целях обеспечения миссии по ликвидации цифровой безграмотности, что также предусмотрено названной национальной программой, разъяснена этимология и значение термина «майнинг», приведены различные доктринальные трактовки данного понятия. Для лучшего понимания сопряженной с майнингом технологии блокчейн представлены ее аналогии с публичной бухгалтерской книгой, ДНК, слоеным пирогом. Раскрыты материально-технические и организационные основы майнинга. Показаны преимущества и недостатки соло-майнинга, майнинга через пулы и облачного майнинга. Представлены результаты компаративистского мониторинга отношения к признанию криптовалюты средством платежа. Обращено внимание на либеральное правовое регулирование технологии блокчейн и майнинга законодательством Республики Беларусь. Показаны этапы законотворческого процесса, направленного на правовое обеспечение майнинга в России. По результатам сопоставления понятий предпринимательской деятельности и майнинга*

¹ Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16081 «Трансформация концептуальных основ подготовки юристов для сферы бизнеса в условиях цифровой экономики». Авторы выражают признательность генеральному директору ООО «Бутик информационных технологий», кандидату химических наук Н. А. Троицкому, выступившему в качестве ИТ-консультанта публикации.

© Ершова И. В., Трофимова Е. В., 2019

* *Ершова Инна Владимировна*, заведующий кафедрой предпринимательского и корпоративного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, профессор, заслуженный юрист Российской Федерации
inna.ershova@mail.ru

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

** *Трофимова Елена Валерьевна*, доцент кафедры предпринимательского и корпоративного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), кандидат юридических наук

trafica@yandex.ru

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

сделан вывод о том, что майнинг — один из новых видов предпринимательства, вызванный к жизни потребностями цифровой экономики. Высказано предложение о признании субъектов майнинга самозанятыми лицами. Отмечено, что предпринимательский характер майнинговой деятельности обуславливает вопросы о мерах ее государственного регулирования, которое затруднительно в рамках сложившейся парадигмы, но которое должно строиться на основе баланса частных и публичных интересов.

Ключевые слова: майнинг, блокчейн, криптовалюта, биткоин, цифровая экономика, цифровая грамотность, предпринимательская деятельность, самозанятые лица, законотворческий процесс, национальная программа, федеральный проект.

DOI: 10.17803/1994-1471.2019.103.6.073-082

Научно-технический прогресс неизбежно приводит к появлению новых видов социальной активности. Их принятие обществом, понимание содержания и целей — не всегда простой и быстротечный процесс. Четвертая промышленная революция, развернувшаяся на наших глазах, указанные процессы активизировала. Цифровизация экономики и сопряженные с ней изменения требуют от юристов, на наш взгляд, гораздо больших, чем ранее, усилий. Почему? Ответ очевиден. Практически все мы, гуманитарии, в лучшем случае «продвинутые пользователи» различных технических устройств. В базовые программы подготовки юристов, в том числе кадров высшей квалификации, не входила, да зачастую и не входит, «цифровая грамотность». Мало таких программ предлагается и в системе дополнительного образования. Поэтому переход от «образования на всю жизнь» к «образованию через всю жизнь» становится более чем актуальным.

У читателя может возникнуть вопрос: почему статья о таком явлении, как майнинг, начинается с пространных рассуждений о необходимости непрерывного образования. Да потому, что задача юристов видится в осмыслении активно происходящих в обществе новых процессов, выявлении их правовой природы, определении направлений (а в идеале — и предвидения) правового обеспечения. Требуется формирование нормативного регулирования цифровой

среды — именно так называется федеральный проект, входящий в структуру национальной программы «Цифровая экономика Российской Федерации»². Срок реализации указанного проекта весьма ограниченный — до 31 декабря 2021 г. Заметим, что на момент написания данной статьи реализация проекта в аспекте рассматриваемой проблемы уже несколько «пробуксовывала».

Выступая 17 сентября 2018 г. на заседании президиума Совета при Президенте РФ по стратегическому развитию и национальным проектам, Д. А. Медведев подчеркнул: «Первое, над чем нужно будет работать в рамках нацпроекта, — это современное регулирование. В нашей стране должны появиться благоприятные и конкурентные условия для участников цифровой среды, а также единые требования по различным электронным операциям, будь то процесс идентификации, оборот документов или хранение и обработка данных. Я неоднократно говорил о том, что касается регулирования: регулирование должно быть экономичным. Мы не должны ставить перед собой цель все зарегулировать, потому что в противном случае это будет сдерживающим фактором, а не стимулом к развитию цифровых технологий. Иными словами, регулирование здесь должно быть необходимым и достаточным»³. Как тут не вспомнить, что условия «необходимости» и «достаточности» используются в логике и ма-

² Паспорт национальной программы «Цифровая экономика Российской Федерации», утвержден Президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 24 декабря 2018 г. № 16 // URL: <http://static.government.ru/media/files/urKHm0gTPPnzJlaKw3M5cNLo6gczMkPF.pdf> (дата обращения: 23 марта 2019 г.).

тематике для обозначения видов связи суждений⁴. Думается, что в аспекте правового поля цифровой экономики это весьма символично.

Итак, вернемся к майнингу.

ЛИКБЕЗ, ИЛИ ЧТО ТАКОЕ МАЙНИНГ

Уверены, что большинство читателей журнала осведомлено о содержании майнинг-деятельности. Однако, выполняя миссию ликвидации цифровой безграмотности, представим краткие сведения о рассматриваемом явлении.

Термин «майнинг» происходит от англ. *mining* — «добыча». Показательно, что при обращении авторов статьи с соответствующим поисковым запросом в научной электронной библиотеке *eLibrary.ru* в качестве результата на первой странице было выдано около 100 статей, посвященных угольной промышленности, в частности Международной специализированной выставке технологий горных разработок «Уголь и майнинг России» (к слову, имеющей более чем 20-летнюю историю). Данный факт не вызывает удивления, если принимать во внимание этимологию слова «майнинг». Также заметим, что нет оснований соотносить этот термин только лишь с «цифровой» проблематикой. В научном обиходе он давно прижился: например, *data mining*, или добыча данных, — технология извлечения необходимой для исследования информации из разнородных, порой неструктурированных источников, — уже многие годы стоит на вооружении исследователей рынков, биржевых аналитиков, фармацевтических компаний и медиков. Вместе с тем термин «майнинг» сегодня наполняется новым содержанием.

Применительно к проблематике нашего исследования авторами научных публикаций не-

однократно предпринимались весьма удачные попытки трактовки рассматриваемого понятия. Объясним и тот факт, что трактовка майнинга, как правило, сопровождается разъяснениями специфики технологии блокчейн.

Так, Е. И. Щедрина указывает, что «майнинг — это создание криптовалют по специальному алгоритму. При этом в компьютере генерируется уникальный набор данных (также называемый блоком), который подтверждает достоверность платежных транзакций. Блок состоит из хеша заголовка предыдущего блока, хеша транзакций и случайного числа»⁵. Майнинг и блокчейн имеют несколько характерных особенностей: в системе виртуальной валюты нет централизованного управления; пользователи данной сети не обязаны предоставлять официальные персональные данные; майнинг работает по первоначально заданным алгоритмам, невозможно произвести больше криптовалюты, чем положено⁶.

А. Г. Гаврилов, И. Ю. Арзина разъясняют, что «майнинг — это способ получения новых блоков (монет) криптовалюты посредством решения компьютером определенных криптографических, математических и других видов вычислений. Это приносит определенное количество электронных денег, которые вносятся в общую копилку и регистрируются в публичной «бухгалтерской книге» (*blockchain*)»⁷. Обратим внимание на удачное, на наш взгляд, сравнение технологии блокчейн (от англ. *block chain* — цепочка блоков) с публичной бухгалтерской книгой. Убеждены, что задачу ликвидации цифровой безграмотности населения можно решить лишь таким образом — проводя аналогии традиционных явлений и процессов с теми, которые еще нуждаются в понимании. Действительно, блокчейн — это цепь, содержащая в себе все

³ URL: <http://government.ru/news/34001/> (дата обращения: 23 марта 2019 г.).

⁴ Эдельман С. Л. Математическая логика. М.: Высшая школа, 1975. С. 26, 30.

⁵ Щедрина Е. И. Криптовалюта как новый специфический вид денег // Проблемы и перспективы развития России: Молодежный взгляд в будущее: сб. научных статей Всероссийской научной конференции. Курск, 2018. Т. 1. С. 327.

⁶ Майнинг криптовалюты // URL: <https://miningcryptocurrency.ru/что-такое-майнинг-криптовалюты/> (дата обращения: 23 марта 2019 г.).

⁷ Гаврилов А. Г., Арзина И. Ю. Майнинг криптовалюты // Аллея науки. 2017. Т. 2. № 16. С. 356.

последовательные транзакции, по записям в блокчейне можно отследить все монеты и узнать баланс любого кошелька. Чем не аналог (хотя и весьма условный) бухгалтерского учета с его принципами, хорошо известными из нормативных правовых актов и литературы?⁸

Справедливости ради отметим и иные, может быть, более понятные читателю аналогии. Так, некоторые авторы предлагают сравнивать технологию блокчейн с ДНК человека. К примеру, Д. Р. Газетдинова и З. Р. Шарифьянова отмечают: «Если проводить сравнение, то вся сеть устройств — это организм, каждое устройство подобно клетке, а база данных — ДНК. Клетки несут в себе информацию обо всем организме в зашифрованном виде. Только, в отличие от ДНК, база данных в блокчейне постоянно пополняется новыми записями. Она хранится на большом количестве устройств, расположенных по всему миру, и имеет открытый доступ для просмотра»⁹. Эти устройства называются «майнерами» и «нодами» (от лат. *nodus* — узел).

По своей сути как блокчейн, так и криптовалюта являются цифровым механизмом распределения прав владения неким активом по установленным правилам, а также способом совершения транзакций (сделок) с этими правами. В случае, например, ICO — InitialCoinOffer (своего рода аналог IPO — первичного размещения акций на рынке ценных бумаг, но только в мире криптовалют) разделяемым активом является участие в размещающейся компании. Большинство криптовалют представляют собой отлаженный способ разрезания «пирога» на куски и обмена кусками, но без реального обеспечения в виде собственно «пирога». Рыночная стоимость одного биткоина определяется, таким образом, всего лишь степенью доверия к этому способу деления «пирога» в расчете на то, что «пирог» будет выпечен.

Рассмотренные выше особенности технологии блокчейн нашли отражение в определении, закрепленном в приложении 1 к Декрету Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики»¹⁰, согласно которому майнинг — это отличная от создания собственных цифровых знаков (токенов) деятельность, направленная на обеспечение функционирования реестра блоков транзакций (блокчейна) посредством создания в таком реестре новых блоков с информацией о совершенных операциях. Лицо, осуществляющее майнинг, становится владельцем цифровых знаков (токенов), возникших (добытых) в результате его деятельности по майнингу, и может получать цифровые знаки (токены) в качестве вознаграждения за верификацию совершения операций в реестре блоков транзакций (блокчейне).

МАТЕРИАЛЬНО-ТЕХНИЧЕСКИЕ И ОРГАНИЗАЦИОННЫЕ ОСНОВЫ МАЙНИНГОВОЙ ДЕЯТЕЛЬНОСТИ

Осуществлять майнинговую деятельность сегодня может любой человек, обладающий знаниями на уровне продвинутого пользователя ПК. Для этого необходимы материальное оснащение в виде компьютера с большой вычислительной мощностью или специализированного оборудования, которое широко доступно на рынке, и набор соответствующего программного обеспечения, реализующий алгоритмы собственно майнинга и сопряжение с экосистемой (кошельком и распределенной бухгалтерской книгой) искомой криптовалюты. Имущественный комплекс для производства криптовалюты, представляющий собой совокупность перечисленных выше составляющих, в ИТ-среде получил название «фермы» для майнинга криптовалют (Cryptomining Farm). Однако

⁸ См.: Предпринимательское право. Правовое сопровождение бизнеса : учебник для магистров / отв. ред. И. В. Ершова. М. : Проспект, 2017. С. 566— 571.

⁹ Газетдинова Д. Р., Шарифьянова З. Р. Биткоин, майнинг и блокчейн: будущее криптовалют в России // Современная экономика: актуальные вопросы, достижения и инновации : сб. статей XXIII Междунар. науч.-практ. конференции : в 2 ч. / отв. ред. Г. Ю. Гуляев. Пенза, 2018. С. 160—161.

¹⁰ Национальный правовой интернет-портал Республики Беларусь. URL: <http://pravo.by/document/?guid=12551&p0=Pd1700008&p1=1&p5=0> (дата обращения: 30 марта 2019 г.).

сегодня, чтобы продуктивно «майнить», порой нужны колоссальные мощности — в этой области преуспевают даже не отдельные фермы, а целые майнинговые вычислительные центры, состоящие из сотен и тысяч подобных ферм.

Для эффективного (но и весьма затратного) майнинга используют интегральные схемы особого назначения — ASIC (от англ. application-specific integrated circuit, интегральная схема специального назначения), предназначенные для решения только рассматриваемой конкретной задачи и почти непригодные для иного применения. Отдельные видеокарты могут, помимо собственно отрисовки графики в компьютерных играх, выполнять сложные расчеты, присовокупляя мощь своих процессорных ядер к основному процессору ПК. Это позволяет выполнять некоторые вычисления (и в том числе майнинг) в сотни раз быстрее, чем способен даже самый мощный ПК сам по себе. Отличаются методы шифрования, применяемые для производства различных криптовалют. Так, Scrypt используется в качестве PoW (Proof-of-Work, «подтверждение работой») в криптовалютах Litecoin, Worldcoin; SHA-256 — при добыче биткоин.

На практике существуют различные способы организации майнинговой деятельности. Это:

- соло-майнинг, при котором майнер добывает криптовалюту самостоятельно. На ранних этапах становления криптовалют это был основной вид майнинга, когда добычу криптовалюты выполняли энтузиасты по всему миру;
- майнинг через пулы (от англ. pool — бассейн) — это серверы, которые могут объединять мощности персональных компьютеров многих майнеров. Интернет пестрит объявлениями, в которых предлагается отдать мощность своего компьютера в ночное время для майнинга. Для этого предлагается поставить на компьютер приложение, которое сочетает в себе кошелек криптовалюты и позволяет серверу использовать ПК пользователя как один из множества узлов рас-

пределенной вычислительной сети. Однако в ряде случаев контроль внешнего сервера над ПК доверчивого пользователя может идти намного дальше вычислений криптоблоков;

- облачный майнинг, при котором майнер платит деньги какой-либо компании за оборудование, после чего данная компания берет на себя ответственность за установку оборудования и его настройку для работы¹¹. По сути, в данном случае речь идет об аренде имеющихся мощностей. Владелец оборудования окупает капиталовложения в него, обеспечивает арендатора необходимой вычислительной инфраструктурой, а тот, используя предоставленную инфраструктуру, получает свою криптовалюту.

Каждый из указанных видов организации майнинговой деятельности имеет свои достоинства и недостатки. Так, при соло-майнинге все добытые в блоке монеты не подлежат разделу, как это происходит в пуле. Однако в случае майнинга через пулы повышается вероятность нахождения блока. Неоспоримыми преимуществами облачного майнинга являются отсутствие необходимости в специальных знаниях и возможность получить доступ к оборудованию, не приобретая его самостоятельно и не выполняя настройку, а также не тратя ресурсы на поддержку оборудования в работоспособном состоянии. Однако при закрытии компании, предоставляющей облачный майнинг, как правило, вернуть вложенные средства не представляется возможным.

При использовании любого из обозначенных видов майнинга очевидно, что речь идет о реальных инвестициях — это как купить станок и изготавливать на нем продукцию. Следовательно, справедливо отмечают специалисты, здесь есть такие понятия, как амортизация, физический и моральный износ, прочие производственные издержки (например, потребление электроэнергии)¹². Добавим сюда такие эконо-

¹¹ Подробнее см.: *Terper A. Bitcoin — The People's Money*, 2016. 59 p.

¹² *Петухов Э. Э. Черкашнев Р. Ю. Майнинг как основа деятельности на криптовалютном рынке // Актуальные проблемы развития финансового сектора : материалы V Междунар. науч.-практ. конференции. Тамбов, 2017. С. 713.*

мико-правовые категории и явления, как срок окупаемости, конкуренция, — и, бесспорно, получим экономическую деятельность.

ПРАВОВОЕ ОФОРМЛЕНИЕ МАЙНИНГА: ЗАКОНОТВОРЧЕСКАЯ ИСТОРИЯ ПРОДОЛЖАЕТСЯ

Проблематика правового оформления майнинговой деятельности неразрывно связана с отношением государства к признанию криптовалюты законным средством платежа. Известно, что в настоящее время биткоинами можно расплачиваться за цифровые товары и услуги — например, такие возможности предоставляет компания WordPress¹³, программное обеспечение которой используют 33 % всех сайтов мира. Биткоин и иная криптовалюта принимаются к оплате на онлайн-аукционах и в интернет-магазинах. Форекс-брокеры создали инструменты для работы с криптовалютами. Некоторые платежные системы (WebMoney и др.), работают с криптографическими валютами и даже создали для них кошельки. Участники процесса открыто обсуждают проблемы необходимости правового регулирования криптовалюты (Cryptocurrency regulation¹⁴) на форумах.

Наблюдается разное отношение к законности указанного явления в зарубежных странах — от признания биткоина легальным средством платежа (Япония), обложения налогом как имущества (США), признания частными (Германия), фиатными (Евросоюз) деньгами как договорного средства платежа до запрета размещения и проведения официальных операций (Китай). Поскольку анализ законности использования биткоинов и иной криптовалюты (Litecoin, Ripple, Ethereum, NEM, Stratis, Bitshares и др.) не является целью данной статьи, лишь отметим,

что в научных и публицистических исследованиях представлены результаты компаративистского мониторинга по данной проблеме¹⁵.

В России попытка законодательной регламентации майнинговой деятельности была предпринята в вынесенной на первое чтение редакции проекта федерального закона № 419059-7 «О цифровых финансовых активах»¹⁶. Названный документ закреплял в ст. 2 основные понятия, трактуя майнинг как деятельность, направленную на создание криптовалюты и/или валидацию с целью получения вознаграждения в виде криптовалюты. Майнинг, было указано в законопроекте, признается предпринимательской деятельностью в случае, когда лицо, которое его осуществляет, в течение трех месяцев подряд превышает лимиты энергопотребления, установленные Правительством РФ.

Таким образом, разработчики закона предлагали свое видение майнинга как предпринимательства при условии его осуществления как деятельности. Обратим внимание на то, что О. М. Олейник совершенно справедливо в качестве первого критерия квалификации предпринимательской деятельности выделяет признак ее ведения именно как «деятельности», характеризующейся систематичностью осуществления; постоянством, длительностью осуществления операций; целенаправленностью¹⁷.

Помимо этого, разработчики принятого в первом чтении законопроекта построили квалификацию майнинга как предпринимательства и на признаке использования энергетических мощностей, что также вполне вписывается в представленную в научной литературе систему признаков предпринимательской деятельности¹⁸.

При подготовке ко второму чтению профильным Комитетом Государственной Думы по

¹³ URL: <https://ru.wordpress.org/> (дата обращения: 29 марта 2019 г.).

¹⁴ URL: <https://bitcointalk.org/index.php?topic=2036590.0> (дата обращения: 29 марта 2019 г.).

¹⁵ URL: <https://cryptomagic.ru/regulirovanie/majning-zakonno-li-eto.html> (дата обращения: 23 марта 2019 г.).

¹⁶ URL: <http://sozd.duma.gov.ru/bill/419059-7> (дата обращения: 29 марта 2019 г.).

¹⁷ Олейник О. М. Формирование критериев осуществления предпринимательской деятельности в судебной практике // Предпринимательское право. 2013. № 1. С. 4—5.

¹⁸ Ершова И. В. Понятие предпринимательской деятельности в теории и судебной практике // Lex Russica. 2014. № 2. С. 160—167.

финансовому рынку была проведена большая аналитическая работа. Среди поправок, касающихся нашего исследования, обратим внимание на следующие. Депутат М. В. Щапов предлагал определить майнинг как деятельность, направленную на создание криптовалюты и/или обеспечение функционирования реестра блоков транзакций (блокчейна) посредством создания в таком реестре новых блоков с информацией о совершенных операциях. Автор поправки полагал необходимым закрепить, что майнинг признается предпринимательской деятельностью в случае, когда лицо, которое его осуществляет (майнер) получает прибыль в виде рублей или иностранной валюты.

Согласно поправке депутата А. Г. Кобилева, майнинг предлагалось определить как предпринимательскую деятельность индивидуальных предпринимателей или юридических лиц, зарегистрированных в налоговых органах, направленную на создание криптовалюты и/или валидацию с целью получения вознаграждения в виде криптовалюты.

Как следует из процитированного, авторы указанных поправок в качестве признака майнинга как предпринимательской деятельности предусматривали его возмездный характер — как результат либо цель деятельности. Данные поправки были отклонены Комитетом по финансовому рынку, а из текста законопроекта № 419059-7, размещенного на официальном сайте Государственной Думы ко второму чтению¹⁹, статья, содержащая понятийный аппарат, по предложению депутатов А. Г. Аксакова и О. А. Николаева была исключена.

В целом документ, предложенный ко второму чтению, претерпел существенные изменения. Было изменено и концептуальное понимание майнинг-деятельности. Из предпринимательской деятельности по «до-

быче криптовалют» данная деятельность превратилась, по сути, в выпуск цифровых финансовых активов.

Очевидно, что такая мощная законодательная пертурбация имеет под собой веские причины. Некоторые из них объяснены в официальном отзыве Правительства РФ на законопроект № 419059-7. Правительство считает, говорится в отзыве, что деятельность, направленная на создание криптовалюты, может не быть напрямую связана с формированием реестра транзакций, а может заключаться в предоставлении энергетических, технических мощностей, в том числе площадей, на которых размещается необходимое для майнинга оборудование, в связи с чем такая деятельность не может быть отнесена к майнингу. С учетом изложенного Правительство полагает необходимым уточнить определение предлагаемого понятия «майнинг». Правительство также посчитало целесообразным расширить перечень критериев, на основании которых субъект может быть признан лицом, осуществляющим майнинг, поскольку показатель энергопотребления не дает однозначного основания для такого вывода²⁰.

Другие причины, побудившие пересмотреть текст законопроекта, кроются в появлении Федерального закона от 18 марта 2019 г. № 34-ФЗ «О внесении изменений в части первую, вторую и ст. 1124 части третьей Гражданского кодекса Российской Федерации»²¹. Данный Закон, отнеся цифровые права к объектам гражданских прав, квалифицировал их в качестве имущественных прав в составе «иного имущества». Показательно в связи с этим, что законопроект № 419059-7 был перенесен для рассмотрения во втором чтении на будущий период — очевидно, для более полной корреляции с положениями Федерального закона от 18 марта 2019 г. № 34-ФЗ.

¹⁹ URL: <http://sozd.duma.gov.ru/bill/419059-7> (дата обращения: 29 марта 2019 г.).

²⁰ URL: <https://government.ru/activities/selection/303/32374/> (дата обращения: 29 марта 2019 г.).

²¹ URL: <http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102528600> (дата обращения: 29 марта 2019 г.).

ВМЕСТО ЗАКЛЮЧЕНИЯ, ИЛИ ПРАВОВАЯ ПРИРОДА МАЙНИНГА

Примером либерального подхода к регулированию майнинга являются положения Декрета Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики», согласно которым деятельность по майнингу, осуществляемая физическими лицами самостоятельно без привлечения иных физических лиц по трудовым и (или) гражданско-правовым договорам, не является предпринимательской деятельностью, а также не требует получения специального разрешения (лицензии) на осуществление деятельности по технической и (или) криптографической защите информации. До 1 января 2023 г. доходы физических лиц от деятельности по майнингу не признаются объектом налогообложения подоходным налогом.

Тем не менее при осуществлении правовой квалификации майнинга представляется необходимым руководствоваться признаками, имманентно присущими рассматриваемому явлению, а потому не зависящими от намерения регулятора придать этой деятельности наиболее простую и удобную форму.

Самостоятельный и рисковый характер указанной деятельности, позволяющей систематически получать прибыль от использования вычислительной техники для обеспечения функционирования реестра блоков транзакций (блокчейна), дает основание прийти к выводу о том, что майнинг — один из новых видов предпринимательства, вызванный к жизни потребностями цифровой экономики. Подобная квалификация тем не менее не исключает из числа субъектов майнинга самозанятых лиц²², которым, помимо уведомительного порядка легитимации, могут быть также предоставлены налоговые каникулы.

Предпринимательский характер данной деятельности обуславливает вопросы о мерах ее государственного регулирования, которое затруднительно осуществлять в рамках сложившейся парадигмы. При этом майнинг является лишь одним из элементов системы отношений, возникающих в связи с использованием блокчейна бизнесом, обществом и государством, механизмы регулирования которого должны не только обеспечивать стабильность финансовой системы и противодействие легализации (отмыванию) доходов, полученных преступным путем, но и защищать права пользователей информационных технологий.

БИБЛИОГРАФИЯ

1. Гаврилов А. Г., Арзина И. Ю. Майнинг криптовалюты // *Аллея науки*. — 2017. — Т. 2. — № 16. — С. 355—361.
2. Газетдинова Д. Р., Шарифьянова З. Р. Биткоин, майнинг и блокчейн: будущее криптовалют в России // *Современная экономика: актуальные вопросы, достижения и инновации* : сборник статей XXIII Международной научно-практической конференции : в 2 ч. / отв. ред. Г. Ю. Гуляев. — Пенза, 2018. — С. 159—162.
3. Ершова И. В. Понятие предпринимательской деятельности в теории и судебной практике // *Lex Russica*. — 2014. — № 2. — С. 160—167.
4. Ершова И. В., Трофимова Е. В. Самозанятость: реперные точки формирования правового режима // *Предпринимательское право*. — 2017. — № 3. — С. 3—12.
5. Олейник О. М. Формирование критериев осуществления предпринимательской деятельности в судебной практике // *Предпринимательское право*. — 2013. — № 1. — С. 2—16.

²² Ершова И. В., Трофимова Е. В. Самозанятость: реперные точки формирования правового режима // *Предпринимательское право*. 2017. № 3. С. 12.

6. Петухов Э. Э. Черкашнев Р. Ю. Майнинг как основа деятельности на криптовалютном рынке // Актуальные проблемы развития финансового сектора : материалы V международной научно-практической конференции. — Тамбов, 2017. — С. 713—723.
7. Предпринимательское право. Правовое сопровождение бизнеса : учебник для магистров / отв. ред. И. В. Ершова. — М. : Проспект, 2017. — 848 с.
8. Щедрина Е. И. Криптовалюта как новый специфический вид денег // Проблемы и перспективы развития России : Молодежный взгляд в будущее : сборник научных статей Всероссийской научной конференции. — Курск, 2018. — Т. 1. — С. 326—328.
9. Эдельман С. Л. Математическая логика. — М. : Высшая школа, 1975. — 176 с.
10. *Tepper A.* Bitcoin — The People's Money, 2016. — 59 p.

Материал поступил в редакцию 6 мая 2019 г.

MINING AND BUSINESS ACTIVITIES: IN SEARCH OF THE BALANCE²³

ERSHOVA Inna Vladimirovna, Head of the Department of Business and Corporate Law of the Kutafin Moscow State Law University (MSAL), Doctor of Law, Professor, Honored Lawyer of the Russian Federation
inna.ershova@mail.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

TROFIMOVA Elena Valerevna, PhD in Law, Associate Professor of the Department of Business and Corporate Law of the Kutafin Moscow State Law University (MSAL)
trafica@yandex.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

Abstract. *The article reveals the content and outlines approaches to the definition of the legal nature of mining. Attention is drawn to the necessity of legal regulation of this activity, which is predetermined by the Federal Program «Digital Economy of the Russian Federation» — a project that provides for normative regulation of the digital environment. In order to support the mission to eliminate digital illiteracy, which is also envisaged in the National Program, the author elucidates the etymology and meaning of the term «mining» and considers various doctrinal interpretations of this concept. The paper presents such analogies of the blockchain technology as the public ledger, DNA, and a layer-cake for a better understanding of the blockchain technology that is associated with mining. Material-technical and organizational foundations of mining are revealed. The author demonstrates advantages and disadvantages of solo mining, pool mining, and cloud mining. The results of comparative monitoring of the attitude to the recognition of cryptocurrency as a means of payment are presented. Attention is drawn to the liberal legal regulation of blockchain technology and mining under the laws of the Republic of Belarus. The paper determines the stages of a law-making process aimed at legal support of mining in Russia. Based on the results of comparison of concepts of entrepreneurial activity and mining, it is concluded that mining represents one of new types of entrepreneurship brought to life due to the needs of digital economy. The author suggests that mining participants be recognized as self-employed persons. It is noted that the entrepreneurial nature of mining*

²³ The study was carried out with the financial support of RFBR within the framework of the scientific project No. 18-29-16081 «Transformation of the Conceptual Foundations of Training Lawyers for the Area of Business in the Digital Economy.» The authors express their gratitude to N.A. Troitskiy - Director General of LLC «Boutique of Information Technologies,» PhD in Chemical Sciences who acted as an IT consultant of the publication

arises questions concerning measures of its state regulation which is difficult within the framework of the existing paradigm, but should be built on the basis of a balance between private and public interests.

Keywords: *mining, blockchain, cryptocurrency, bitcoin, digital economy, digital literacy, entrepreneurial activity, self-employed persons, law-making process, national program, federal project.*

REFERENCES (TRANSLITERATION)

1. Gavrilov A. G., Arzina I. Yu. Majning kriptovalyuty // *Alleya nauki*. — 2017. — T. 2. — № 16. — S. 355—361.
2. Gazetdinova D. R., Sharif'yanova Z. R. Bitkoin, majning i blokchejn: budushchee kriptovalyut v Rossii // *Sovremennaya ekonomika: aktual'nye voprosy, dostizheniya i innovacii : sbornik statej XXIII Mezhdunarodnoj nauchno-prakticheskoy konferencii : v 2 ch. / otv. red. G. Yu. Gulyaev*. — Penza, 2018. — S. 159—162.
3. Ershova I. V. Ponyatie predprinimatel'skoj deyatel'nosti v teorii i sudebnoj praktike // *Lex Russica*. — 2014. — № 2. — S. 160—167.
4. Ershova I. V., Trofimova E. V. Samozanyatost': repertnye tochki formirovaniya pravovogo rezhima // *Predprinimatel'skoe pravo*. — 2017. — № 3. — S. 3—12.
5. Olejnik O. M. Formirovanie kriteriev osushchestvleniya predprinimatel'skoj deyatel'nosti v sudebnoj praktike // *Predprinimatel'skoe pravo*. — 2013. — № 1. — S. 2—16.
6. Petuhov E. E., Cherkashnev R. Yu. Majning kak osnova deyatel'nosti na kriptovalyutnom rynke // *Aktual'nye problemy razvitiya finansovogo sektora : materialy V mezhdunarodnoj nauchno-prakticheskoy konferencii*. — Tambov, 2017. — S. 713—723.
7. *Predprinimatel'skoe pravo. Pravovoe soprovozhdenie biznesa : uchebnyk dlya magistrrov / otv. red. I. V. Ershova*. — M. : Prospekt, 2017. — 848 s.
8. Shchedrina E. I. Kriptovalyuta kak novyj specificheskij vid deneg // *Problemy i perspektivy razvitiya Rossii : Molodezhnyj vzglyad v budushchee : sbornik nauchnyh statej Vserossijskoj nauchnoj konferencii*. — Kursk, 2018. — T. 1. — S. 326—328.
9. Edel'man S. L. *Matematicheskaya logika*. — M. : Vysshaya shkola, 1975. — 176 s.

М. А. Егорова*

Биткоин как особый вид криптовалюты: понятие, значение и перспективы правового регулирования в предпринимательской деятельности¹

Аннотация. В целях развития цифровой экономики в Российской Федерации распоряжением Правительства РФ от 28.07.2017 № 1632-р утверждена Программа «Цифровая экономика Российской Федерации», которая направлена в том числе на формирование нормативной базы для правового регулирования новых отношений в сфере цифровой экономики. Особенно актуальным в связи с этим является вопрос правового регулирования криптовалюты и биткоина. В статье подробно рассматривается особый вид криптовалюты — биткоин. Анализируются основные проблемы, связанные с необходимостью правового регулирования криптовалют, делается вывод о том, что правовое регулирование криптовалюты как средства платежа требует комплексного подхода и невозможно без учета особенностей правового регулирования биткоина. Приводится соотношение понятия биткоина с иными ключевыми понятиями: виртуальная валюта и цифровая валюта. Делается вывод о необходимости создания в целях защиты интересов криптовалютного бизнеса негосударственной саморегулируемой организации, имеющей поддержку со стороны государства. Поскольку вопрос правового регулирования криптовалют носит глобальный характер, в статье исследован зарубежный опыт правового регулирования криптовалют и их видов.

Ключевые слова: криптовалюта, биткоин, цифровая экономика, фиатные валюты, платежное средство, валюта, государственное регулирование, стимулирующие меры.

DOI: 10.17803/1994-1471.2019.103.6.083-089

Российская Федерация последние два года активно вовлечена в процесс формирования правовых режимов, которые могут составить основу будущего нормативного регулирования в сфере цифровой экономики. Такие основы заложены в Программе цифровой

¹ Статья подготовлена в рамках проведения исследования на средства гранта Российского фонда фундаментальных исследований (РФФИ) в рамках научного проекта № 18-29-16056 «Криптовалюта как средство платежа частноправовой и налоговый аспекты».

© Егорова М. А., 2019

* *Егорова Мария Александровна*, доктор юридических наук, профессор кафедры конкурентного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), заместитель председателя исполнительного комитета и председатель комиссии по совершенствованию антимонопольного законодательства Московского отделения Ассоциации юристов России, сопresident Международного союза юристов и экономистов (Франция), член Международного комитета цифровой экономики (БРИКС)

Lab.kkonkpr@msal.ru

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

экономики², утвержденной Правительством РФ в 2017 г.

Одним из основных направлений совершенствования правового регулирования в сфере цифровой экономики в этой Программе названо государственное регулирование криптовалютной деятельности. Технология блокчейн стала наиболее распространенной благодаря использованию биткоина, который является сейчас основной криптовалютой. Впервые понятие биткоина и соответствующая блокчейн-технология были представлены более 10 лет назад, в 2008 г., Сатоши Накамото в статье «Биткоин: электронная пиринговая денежная система»³.

В настоящее время на использование криптовалюты в России установлен абсолютный запрет. Это обусловлено различными факторами. В частности, введение криптовалюты как средства платежа может подорвать, по мнению многих экспертов, денежный оборот в стране и проявиться в исчезновении монополии Центрального банка. Российскому законодателю в ближайшее время необходимо решить вопрос о правовом режиме криптовалюты; так, необходимо с правовой точки зрения определить: является ли криптовалюта товаром, средством платежа или средством обмена? Для примера мы можем обратиться к зарубежному опыту. В ноябре 2015 г. Европейский Суд (European Court of Justice) вынес решение, согласно которому биткоин необходимо считать именно валютой (средством платежа), а не товаром. По крайней мере с точки зрения налогообложения. Таким образом, операции по купле и продаже биткоина за традиционные фиатные валюты не должны облагаться налогом на добавленную стоимость. В Норвегии, Финляндии и Германии криптовалюта облагается налогом на прирост капитала и налогом на роскошь. В Австрии криптовалюта рассматривается налоговыми органами в качестве нематериального актива, а ее майнинг — как операционная деятельность. В США криптовалюты считаются собственно-

стью, все операции с подобной валютой облагаются налогом. В ближайшее время российскому законодателю необходимо определиться, по какому пути должно пойти российское право. В этой связи также представляется необходимым установление правового режима процесса ICO (initial coin offering), представляющим собой процедуру выпуска криптовалюты, продавая которую лицо получает дополнительные средства. В этой части выпуск криптовалюты в рамках ICO очень схож с выпуском облигаций, но в отличие от облигаций криптовалюта, выпущенная компанией или индивидуальным предпринимателем, никаких имущественных прав требования к выпустившему не предполагает, поскольку существует определенный правовой вакуум в этой области. Данный правовой вакуум можно преодолеть законодательно — урегулировав ICO по примеру выпуска ценных бумаг либо урегулировав его на уровне правоприменительной практики, например рассматривая выпуск криптовалюты с публичным предложением как своеобразный способ заключения договора займа.

Одной из основных сфер применения блокчейн-технологии является криптовалюта и платежное средство. Однако технология блокчейна может использоваться и во многих других сферах как способ хранения децентрализованных данных и информации. По своей сути блокчейн представляет собой технологию основанного вида криптовалюты в виде биткоина. Биткоин понимается как технология распределенного реестра, такая технология распределенных реестров является в целом достаточно безопасной и эффективной для возможности ее применения. Суть распределенного реестра, по мнению Л. В. Санниковой и Ю. С. Харитоновой, заключается в том, что распределенный реестр цифровых транзакций представляет собой определенную систематизированную базу цифровых записей, которые децентрализованно хранятся, создаются и обновляются в определенном

² Распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р Об утверждении программы «Цифровая экономика Российской Федерации» // СЗ РФ. 2017. № 32. Ст. 5138.

³ *Nakamoto Satoshi*. A Peer-to-Peer Electronic Cash System // URL: <https://bitcoin.org/bitcoin.pdf> (November, 2008).

режиме⁴. Одним из важнейших направлений развития криптовалюты в современных условиях является потенциальная возможность ее использования не только в качестве средства платежа и обмена, но и как закрепленного в блокчейне права (обязанности), например в качестве «акции» или «векселя».

Не менее важным представляется решение вопроса о том, является ли биткоин и криптовалюта в целом ценной бумагой. Интересными представляются выводы, сделанные Л. Ю. Ефимовой, исследующей зарубежный опыт в указанной сфере. По мнению FINMA, ценными бумагами могут признаваться только инвестиционные токены. В Практическом руководстве содержится определенный вывод о том, что настоящие платежные токены не могут быть квалифицированы как ценные бумаги. Согласно мнению FINMA, такие платежные токены, как Bitcoin или Ethereum, в настоящее время не могут рассматриваться как ценные бумаги⁵.

Все отрасли экономики развитых стран мира все больше вовлечены в процесс формирования правовых режимов криптовалютной деятельности, и в первую очередь это отражается на динамике использования биткоина на товарных рынках. Хозяйствующие субъекты активно используют ресурсы и возможности информационно-коммуникационной сети «Интернет» для продвижения своих товаров, работ, услуг на товарном рынке, и деятельность таких субъектов цифровой экономики должна соответствовать международным стандартам. Свободный обмен информацией, ее перемещение через границы стран и континентов, международная торговля, в том числе интернет-торговля, — это объективная реальность. В этой связи международные договоры в данной сфере должны содержать

единые приемлемые для всех стран стандарты и правила поведения в цифровой среде.

Важным для российского законодательства представляется европейский опыт регулирования криптовалютной деятельности. На первых этапах формирования и развития цифровой экономики в Евросоюзе приоритетной была политика разрешения ICO, если они соответствуют политикам по борьбе с отмыванием денег и «знай своего клиента» (AML/KYC) и основным требованиям к предпринимательской деятельности. Однако уже в ноябре 2017 г. Европейское управление по ценным бумагам и рынкам заняло более жесткую позицию в отношении ICO, указав, что ICO представляет высокий риск для инвесторов, вследствие чего компании, работающим с ICO, должны соответствовать особым нормативным требованиям. Значимым шагом в направлении защиты персональных данных при использовании блокчейн-технологий является Регламент № 2016/679 Европейского парламента и Совета Европейского Союза GDPR (General Data Protection Regulation, Общий регламент по защите данных)⁶.

В январе 2018 г. в Швейцарской Конфедерации ассоциация Crypto Valley Association (CVA) опубликовала Кодекс поведения ICO для Швейцарии⁷, регламентирующий отношения по саморегулированию всех участников оборота криптовалюты. В Великобритании было выпущено предупреждение инвесторам о нерегулируемом характере ICO, при этом Управление по финансовому контролю Великобритании отметило, что даже действуя добросовестно, инвесторы могут потерять все свои деньги в силу пока еще экспериментального характера бизнес-моделей ICO. Аналогичное предупреждение было выпущено и органом по финансовому надзору

⁴ Санникова Л. В., Харитоновна Ю. С. Цифровые активы и технологии: некоторые правовые проблемы выработки понятийного аппарата // Право и цифровая экономика. 2018. № 1. С. 27.

⁵ Цит. по: Ефимова Л. Г. Некоторые аспекты правовой природы криптовалют // Юрист. 2019. № 3.

⁶ Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных). Текст перевода официально опубликован не был; текст Регламента на английском языке опубликован в: OJ, N L 119. 04.05.2016. Pp. 1—88.

⁷ URL: <https://cryptovalley.swiss/>.

Германии, при этом особых нормативных требований в Германии к ICO не имеется, поскольку предполагается распространение на него норм законодательства о банковской деятельности, об инвестициях, о торговле ценными бумагами, о надзоре за платежными услугами и о проспектах эмиссии. В ряде стран (например, в Португалии, Испании, Италии) ICO полностью разрешено, в то время как в Китае и Македонии строго запрещено.

В связи с глубокими противоречиями национальных подходов к регулированию криптовалют говорить о возможности единого глобального регулирования на данном этапе пока затруднительно. В то же время с учетом масштабов распространения биткоина и иных криптовалют практически каждое государство столкнулось с необходимостью так или иначе привести свое законодательство в соответствие с вызовами времени. Полная легализация криптовалют, разрешение их использования с ограничительными условиями, абсолютный запрет — вариантов правового регулирования, как было рассмотрено ранее, множество, и каждое из государств в той или иной форме проводит тщательную работу над определением оптимального регулирования для конкретного государства с учетом всех его особенностей. Многие развитые страны разрабатывают экспертные, межправительственные группы для изучения нормативно-правовой базы виртуальных валют.

Российская Федерация не стала исключением. В целях развития цифровой экономики в Российской Федерации распоряжением Правительства РФ от 28.07.2017 № 1632-р утверждена уже упомянутая выше программа «Цифровая экономика Российской Федерации», которая в том числе направлена на формирование нормативной базы для адекватного регулирования новых отношений, характерных для цифро-

вой экономики. Особенно актуальным в связи с этим является вопрос правового регулирования криптовалюты, и в частности определения сущности данного явления и его места в системе российского права. Правовым режимом криптовалюты должны быть предусмотрены публично-правовые ограничения, которые касаются субъектного состава рассматриваемых отношений, а также прав и обязанностей лиц, использующих криптовалюты (установление видов использования криптовалюты)⁸. Как справедливо отмечает А. В. Михайлов, определенным недостатком криптовалют можно признать отсутствие эмиссионного центра, т.е. классического обеспечения валюты эмитентом⁹.

Прежде чем перейти к вопросу правового регулирования криптовалют и биткоина, необходимо определить, что представляют собой данные явления и чем вызвана необходимость их регулирования. Биткоин, как определил его Р. Гринберг, — это цифровая, децентрализованная, частично анонимная валюта, не поддерживаемая правительством или каким-либо юридическим лицом, не подлежащая обмену на золото или биржевые товары, основанная на одноранговых сетях и криптографии¹⁰.

Следует вывести соотношение понятия биткоина с иными ключевыми понятиями, такими как виртуальная валюта и цифровая валюта. Под виртуальной валютой, как правило, понимаются нерегулируемые цифровые деньги, которые подлежат контролю со стороны их создателей и, как правило, принимаются к оплате в виртуальном мире.

Биткоин представляет собой одноранговую, частную, анонимную и децентрализованную сеть, работающую независимо от банковской системы или правительства. На первый взгляд, биткоин можно признать деньгами, так как он может быть использован для покупки или продаж товаров, для определения меры стоимости.

⁸ Макаrchук Н. В. Публично-правовые ограничения использования криптовалют как способ минимизации возможных рисков цифровизации экономики // Право и цифровая экономика. 2018. № 1. С. 22.

⁹ Михайлов А. В. Проблемы становления цифровой экономики и вопросы развития предпринимательского права // Актуальные проблемы российского права. 2018. № 11. С. 71.

¹⁰ Grinberg R. Bitcoin: An Innovative Alternative Digital Currency // 4 Hastings Science & Technology Law Journal 159, 160.

В настоящее время биткоин используется для оплаты товаров и услуг, однако ограниченное число магазинов по всему миру принимает биткоины к оплате. Во многих финансовых изданиях периодически возникали утверждения о том, что биткоины являются «новым золотом»¹¹. Биткоин не обладает внутренней стоимостью, его ценность может значительно измениться в рекордные сроки, что не позволяет признать эквивалентными эти два явления уже по своей сути.

В целях представления и защиты интересов криптовалютного бизнеса необходимо стимулировать создание негосударственной саморегулируемой организации, имеющей поддержку со стороны государства. Такая организация необходима для упорядочивания криптовалютной деятельности. Учитывая сложность и многообразие возникающих отношений, необходимо понимать, что государство не сможет урегулировать на должном уровне все указанные отношения, в связи с чем основным инструментом регулирования отношений в рамках цифровой экосистемы должны стать инструменты саморегулирования, то есть большинство возникающих отношений должно быть урегулировано самими участниками цифровых экосистем.

Подобная практика активно применяется в Японии, где была создана Японская ассоциация криптовалютного бизнеса, включающая в себя 16 зарегистрированных криптовалютных бирж. Она была аккредитована Агентством финансовых услуг Японии как «сертифицированная бизнес-ассоциация по расчетам с фондами», что позволяет ей устанавливать правила для национальных операций по обмену криптовалютой и принимать меры в случае любых нарушений в этой сфере. Стоит отметить, что данная саморегулируемая организация была создана после кражи на бирже Coincheck на сумму 530 млн долл., которая подчеркнула необходимость регулирования отношений в рамках

цифровой экосистемы и защиты инвесторов от криптомошенников¹².

В США в августе 2018 г. ряд компаний решили создать спонсируемую отраслью саморегулируемую организацию для рынков криптовалют в США — Виртуальную товарную ассоциацию (VCA) — для надзора за виртуальными товарными денежными рынками в целях защиты потребителей и обеспечения целостности этих рынков¹³. Ассоциация в ходе совместной работы с государственными регуляторами и законодательными органами планирует достичь оптимального регулирования на рынках криптовалют, стимулирующего инновации, экономический рост и лидерство США в отрасли.

Вполне вероятно, что другие государства, в том числе Россия, также могут посчитать целесообразным использование института саморегулирования в специфичной сфере отношений цифровой экосистемы. Тем более что с учетом особенностей криптовалют (их децентрализованности и анонимности), представляется затруднительным введение именно государственного регулирования рассматриваемых отношений.

Таким образом, можно сделать вывод о том, что в настоящее время государства имеют определенные возможности для эффективного регулирования отношений в рамках цифровой экосистемы. При этом есть несколько сценариев, в соответствии с которыми будет выстраиваться правовое регулирование (в том числе в России).

Во-первых, биткоин и иные криптовалюты могут быть в дальнейшем полностью запрещены. Это наиболее непрогрессивный вариант, однако он имеет место, так как криптовалюты все еще несут в силу своей специфики большую опасность в качестве инструмента совершения преступлений, начиная с кибермошенничества и заканчивая финансированием терроризма и отмытием денег. Однако формальный за-

¹¹ Is bitcoin the new gold? // URL: <https://www.ccn.com/bitcoin-new-gold>.

¹² Japan Allows Cryptocurrency Industry To Regulate Itself // URL: <https://bitcoinist.com/japan-cryptocurrency-self-regulate/>.

¹³ The Virtual Commodity Association Working Group Has Formed and Is Planning Inaugural Meeting // URL: <https://www.businesswire.com/news/home/20180820005066/en/Virtual-Commodity-Association-Working-Group-Formed-Planning>.

прет криптовалют не означает, что таким образом операции с биткоинами прекратятся фактически, следовательно, данный вариант в любом случае неэффективен.

Во-вторых, с учетом того, что всеобъемлющий государственный контроль над криптовалютами установить все же невозможно, есть вероятность, что многие государства отдадут приоритет институту саморегулирования.

В-третьих, невозможность полного установления государственного контроля над криптовалютами не исключает частичного запрета на определенные операции: например, на оплату биткоинами товаров во избежание случаев

мошенничества; не исключается также возможность внедрения государственного контроля в отдельные сферы, например в налогообложение.

В заключение необходимо отметить, что какой бы подход ни был избран в качестве ключевого, нужно понимать, что регулирование в своем идеальном воплощении должно сочетать в себе как обеспечение публичных интересов путем принятия мер по борьбе с преступлениями с использованием криптовалют, так и защиту интересов частных инвесторов и клиентов валютных бирж и при этом создавать благоприятную почву для роста экономики и развития инноваций.

БИБЛИОГРАФИЯ

1. *Ефимова Л. Г.* Некоторые аспекты правовой природы криптовалют // Юрист. — 2019. — № 3.
2. *Макарчук Н. В.* Публично-правовые ограничения использования криптовалют как способ минимизации возможных рисков цифровизации экономики // Право и цифровая экономика. — 2018. — № 1.
3. *Михайлов А. В.* Проблемы становления цифровой экономики и вопросы развития предпринимательского права // Актуальные проблемы российского права. — 2018. — № 11.
4. *Санникова Л. В., Харитонова Ю. С.* Цифровые активы и технологии: некоторые правовые проблемы выработки понятийного аппарата // Право и цифровая экономика. — 2018. — № 1.
5. *Grinberg R.* Bitcoin: An Innovative Alternative Digital Currency // 4 Hastings Science & Technology Law Journal 159, 160.

Материал поступил в редакцию 6 мая 2019 г.

BITCOIN AS A SPECIAL KIND OF CRYPTOCURRENCY: A CONCEPT, MEANING AND PROSPECTS OF LEGAL REGULATION IN BUSINESS¹⁴

EGOROVA Mariya Aleksandrovna, Doctor of Law, Professor of the Department of Competition Law of the Kutafin Moscow State Law University (MSAL), Vice-Chairman of the Executive Committee and Chairman of the Commission for the Improvement of Antitrust Laws of the Moscow Branch of the Association of Lawyers of Russia, Co-President of the International Alliance of Lawyers and Economists (France), member of the International Committee for Digital Economy (BRICS)
Lab.kkonkpr@msal.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

Abstract. *In order to develop the digital economy in the Russian Federation, the Program «Digital Economy of the Russian Federation» that is aimed, inter alia, at the formation of a regulatory framework for the legal regulation*

¹⁴ The article was prepared within the framework of the research carried out at the expense of the funds of the grant of the Russian Foundation for Fundamental Research (RFBR) under the scientific project No. 18-29-16056 «Cryptocurrency as a Means of Payment: Private Law and Taxation Aspects».

of new relations in the field of digital economy, was approved by the Decree of the Government of the Russian Federation No. 1632-r of July 27, 2017. Particularly relevant in this regard is the issue of cryptocurrency and bitcoin legal regulation. The article deals in detail with a special type of cryptocurrency, namely: bitcoin. The author analyzes the main problems associated with the necessity of legal regulation of cryptocurrencies. The conclusion is made that legal regulation of cryptocurrency as a means of payment requires a complex approach and it is impossible without due regard to the peculiarities of legal regulation of bitcoin. The paper provides for the interaction between the concept of bitcoin and other key concepts, namely: virtual currency and digital currency. The author concludes that it is necessary to create a non-governmental self-regulatory organization supported by the State in order to protect the interests of the cryptocurrency business. Since legal regulation of cryptocurrencies is global in its nature, the article examines the foreign experience of legal regulation of cryptocurrencies and their types.

Keywords: Cryptocurrency, bitcoin, digital economy, fiat currencies, means of payment, currency, state regulation, stimulus measures.

REFERENCES (TRANSLITERATION)

1. Efimova L. G. Nekotorye aspekty pravovoj prirody kriptovalyut // Yurist. — 2019. — № 3.
2. Makarchuk N. V. Publichno-pravovye ogranicheniya ispol'zovaniya kriptovalyut kak sposob minimizacii vozmozhnyh riskov cifrovizacii ekonomiki // Pravo i cifrovaya ekonomika. — 2018. — № 1.
3. Mihajlov A. V. Problemy stanovleniya cifrovoj ekonomiki i voprosy razvitiya predprinimatel'skogo prava // Aktual'nye problemy rossijskogo prava. — 2018. — № 11.
4. Sannikova L. V., Haritonova Yu. S. Cifrovye aktivy i tekhnologii: nekotorye pravovye problemy vyrabotki ponyatijnogo apparata // Pravo i cifrovaya ekonomika. — 2018. — № 1.

ПРАВОВАЯ ОХРАНА РЕЗУЛЬТАТОВ ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Е. С. Гринь*,
А. Г. Королева**

Формирование базовых моделей охраны технологий виртуальной и дополненной реальности в сфере права интеллектуальной собственности¹

***Аннотация.** Развитие цифровых технологий коснулось практически всех сфер деятельности человека. На сегодняшний день среди особо значимых результатов цифровой трансформации экономики выделяют технологии виртуальной и дополненной реальности. Качественный рост данных технологий, а также их активное повсеместное применение порождает немало правовых проблем. Одной из них является определение механизмов охраны технологий виртуальной и дополненной реальности, а также продуктов их использования нормами права интеллектуальной собственности.*

В статье рассматриваются особенности правовой природы технологий виртуальной и дополненной реальности, анализируются понятия виртуальности, виртуальной и дополненной реальности с точки зрения различных подходов, встречаемых в литературе. Раскрываются основные объекты интеллектуальных прав, реализуемые в технологиях виртуальной и дополненной реальности, а также порождаемые ими. Авторами делается вывод о возможности обеспечения охраны рассматриваемых результатов интеллектуальной деятельности и средств индивидуализации основными институтами права интеллектуальной собственности, однако ставится вопрос о необходимости выработки новых моделей по охране результатов творческого труда в рассматриваемой сфере.

¹ Исследование выполнено при финансовой поддержке РФФИ № 18-29-16199 МК «Концепция интеллектуальных прав в сфере технологий виртуальной и дополненной реальностей».

© Гринь Е. С., Королева А. Г., 2019

* Гринь Елена Сергеевна, кандидат юридических наук, доцент, заместитель заведующего кафедрой интеллектуальных прав Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)

esgrin@msal.ru

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

** Королева Анастасия Георгиевна, магистрант кафедры интеллектуальных прав Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)

agkoroleva@msal.ru

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

Ключевые слова: интеллектуальные права, виртуальная реальность, новые технологии, интеллектуальная собственность, авторские права, автор, результаты интеллектуальной деятельности, дополненная реальность, правообладатель, коммерциализация, цифровые технологии.

DOI: 10.17803/1994-1471.2019.103.6.090-097

Стремительное развитие цифровых технологий коснулось практически всех сфер деятельности человека. На сегодняшний день среди особо значимых плодов цифровой трансформации экономики выделяют технологии виртуальной и дополненной реальности. В ближайшем будущем в Российской Федерации планируется внедрение современной цифровой образовательной среды, обеспечение создания которой будет реализовано в том числе с помощью данных инновационных достижений².

Рынок технологий виртуальной и дополненной реальности является одним из самых динамично развивающихся. Согласно статистическому анализу, объем инвестиций в сферу дополненной и виртуальной реальности в России по состоянию на 2016 г. составил 700 млн руб.³

Качественный рост технологий виртуальной и дополненной реальности, а также их активное повсеместное применение порождают немалое количество правовых проблем. Одной из них является определение механизмов охраны данных технологий, а также продуктов их использования нормами права интеллектуальной собственности.

Правовая природа технологий виртуальной и дополненной реальности в науке исследована недостаточно. В связи с этим первостепенной задачей, обусловленной целями настоящего ис-

следования, является разработка понятийного аппарата.

Традиционно под **виртуальной реальностью** (virtual reality, VR) понимается искусственная среда, созданная с помощью программного обеспечения и принимаемая человеком в качестве реальной действительности⁴. Прежде чем рассматривать современное содержание понятия виртуальности, на наш взгляд, необходимо обратить внимание и проанализировать историческое развитие данной категории.

Виртуальность в современном понимании используется в философии, психологии, физике, экономике, геологии, медицине, архитектуре и других сферах. Применение этого понятия настолько многогранно, что «это наводит на мысль о тотальной виртуализации всего и вся — вплоть до метафизических оснований мира в целом»⁵.

Однако в литературе отмечается, что определение понятия *виртуальности* в новом компьютерном значении приводит к «состоянию десемантизации»⁶, в котором оно находится в современном русском языке, а также и в европейских языках. Поэтому в последнее время достаточно трудно «ответить на вопрос о том, что означает виртуальное... в этом и состоит большая тайна «всеобщей виртуализации»»⁷.

В литературе по-разному определяют виртуальность. В словаре С. И. Ожегова виртуальный

² Паспорт национального проекта «Образование» (утвержденный Президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 24.12.2018 № 16) // СПС «КонсультантПлюс».

³ План мероприятий («дорожная карта») Национальной технологической инициативы «Автонет» (приложение № 2 к протоколу заседания президиума Совета при Президенте РФ по модернизации экономики и инновационному развитию России от 24.04.2018 № 1) // СПС «КонсультантПлюс».

⁴ Virtual Reality: Patent Landscape Analysis // https://www.wipo.int/edocs/plrdocs/en/lexinnova_plr_virtual_reality.pdf (дата обращения: 01.04.2019).

⁵ См.: Таратута Е. Е. Философия виртуальной реальности. СПб., 2007. С. 7.

⁶ Таратута Е. Е. Указ. соч. С. 2.

⁷ Таратута Е. Е. Указ. соч. С. 2.

означает несуществующий, но возможный, например виртуальный образ⁸. Толковый словарь Д. Н. Ушакова определяет термин как «пребывающий в скрытом состоянии и могущий проявиться, случиться; возможный»⁹.

Виртуальность с учетом обзора понятий термина и подходов (рассмотренных в ранее упомянутой работе) можно определить как свойство идеального объекта, означающее создание с помощью компьютерных технологий имитации объективной реальности или отображения мира, вымышленного автором.

Дополненная реальность (augmented reality, AR) представляет собой «технология наложения информации в форме текста, графики, аудио и других виртуальных объектов на реальные объекты в режиме реального времени»¹⁰. Данное определение отождествляет дополненную реальность и технологию дополненной реальности. Между тем в литературе можно встретить иные дефиниции дополненной реальности. Так, например, Рональд Азума определяет дополненную реальность в качестве системы, совмещающей виртуальное и реальное, работающей в 3D-измерении и взаимодействующей в реальном времени¹¹. В доктрине также можно столкнуться с идеей, согласно которой дополненная реальность представляет собой виртуальные контекстно-зависимые объекты, введенные в поле восприятия любых сенсорных данных¹².

Дополненную реальность можно рассматривать в качестве созданных техническими средствами виртуальных объектов, взаимодействующих с настоящим миром в режиме реального времени. Под технологией дополненной реальности в настоящей статье будет пониматься, соответственно, совокупность методов и инстру-

ментов, с помощью которых создаются данные объекты.

Отличительной особенностью технологии дополненной реальности является то, что она накладывает виртуальные объекты на окружающую среду. Виртуальная реальность предлагает автономный искусственный мир, в чем заключается главное отличие данной технологии от технологии дополненной реальности. Вместе с тем данным технологиям присущи общие важные с точки зрения интеллектуальной собственности черты. Основная из них — объекты, которые включают в себя технологии виртуальной и дополненной реальности. Данные объекты можно разделить на две группы:

- 1) объекты интеллектуальных прав, благодаря которым формируется технология виртуальной или дополненной реальности;
- 2) продукты использования данных технологий.

Например, в первую группу входят созданные творческим трудом авторов объекты, формирующие виртуальную или дополненную реальность, а также средства индивидуализации, используемые при реализации данных технологий.

Между тем охрана объектов, формирующих технологии виртуальной и дополненной реальности, не может ограничиваться лишь авторским правом.

Вторую группу составляют объекты, полученные пользователями технологий виртуальной и дополненной реальности путем создания или их приобретения. Такие объекты могут отвечать любым целям — как личным, так и коммерческим. В связи с этим на практике возникает ряд вопросов, связанных как с правовой природой продуктов использования рассматриваемых

⁸ См.: Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка. М., 1997.

⁹ Толковый словарь русского языка : в 4 т. / под ред. Д. Н. Ушакова. М. : Гос. ин-т Сов. энцикл., 1935—1940.

¹⁰ Яковлев Б. С., Пустов С. И. История, особенности и перспективы технологии дополненной реальности // Известия ТулГУ. Технические науки. 2013. № 3. С. 479.

¹¹ Azuma R. T. A Survey of Augmented Reality // In Presence: Teleoperators and Virtual Environments. 1997. № 4. P. 355.

¹² См. подробнее.: Гришкун А. В. Терминологические особенности изучения технологии дополненной реальности при обучении информатике // Вестник Московского городского педагогического университета. Серия : Информатика и информатизация образования. 2016. № 4 (38). С. 93.

технологий, так и с проблемой использования данных объектов.

Анализ отечественной и зарубежной практики показывает, что основными **моделями охраны технологий виртуальной и дополненной реальности** являются: авторско-правовая, патентно-правовая, а также модель с применением норм о средствах индивидуализации. Рассмотрим данные модели правовой охраны.

В первую очередь речь пойдет об *авторско-правовой модели охраны*. В целом в настоящее время для охраны объектов авторских прав используются традиционные механизмы авторско-правовой охраны. Под охраной понимается установление нормами права общего режима ценностей, в силу которого носитель права может извлекать выгоды при его осуществлении, т.е. предполагается ненарушение права на произведение, и закон такие меры предоставляет¹³.

В большинстве случаев виртуальная среда формируется благодаря компьютерным играм (мы придерживаемся точки зрения, что они являются сложными объектами авторских прав — мультимедийными продуктами, ст. 1240 ГК РФ). Так, например, технология дополненной реальности реализована в мобильных играх и приложениях (например, игра *Rocket League*, разработанная и изданная компанией Niantic, Inc.).

Ядро технологии виртуальной или дополненной реальности составляет программное обеспечение (software). Например, в Российской Федерации зарегистрировано программное обеспечение для виртуального прототипирования и коллективной работы с цифровыми двойниками изделий¹⁴. Согласно отечественному гражданскому законодательству, данные объекты именуются программами для ЭВМ и охраняются как литературные произведения (ст. 1261 ГК РФ). Подобный режим охраны

соответствует международным нормам (ст. 4 Договора ВОИС по авторскому праву, п. 1 ст. 10 Соглашения ТРИПС)¹⁵.

Основной проблемой, связанной с правовой охраной результатов, создаваемых с помощью технологий виртуальной и дополненной реальности, является использование в рассматриваемых технологиях, помимо программного обеспечения, иных результатов интеллектуальной деятельности, которые отвечают критериям охраноспособности объектов авторских прав. Так, помимо программного обеспечения в рассматриваемых технологиях используются изображения, видео, музыкальные и иные произведения, что подтверждает сложный характер технологий виртуальной и дополненной реальности.

Нередко в рассматриваемых технологиях используются базы данных (п. 2 ст. 1260 ГК РФ). Например, в мобильном приложении Яндекс.Карты (разработчик — Yandex LLC) используются базы данных с картами. Подобным образом реализуется технология дополненной реальности в игре *Rocket League*.

Вопрос об обеспечении охраны продуктов использования в виртуальной и дополненной реальности исследуется в юридической литературе. Так, А. И. Савельев предлагает рассматривать виртуальные объекты в качестве иного имущества (ст. 128 ГК РФ)¹⁶. Между тем вопросы, связанные с охраной таких объектов с точки зрения интеллектуальной собственности, до сих пор не исследованы.

Зачастую разработчики платформ виртуальной реальности создают лишь макет виртуального мира, с помощью которого участники процесса могут создавать новые результаты. Подобная тенденция характерна и для технологии дополненной реальности. Так, например, пользователи социальной сети Instagram могут

¹³ См.: Гринь Е. С. Ты — автор. Что такое авторские и смежные права / под ред. Л. А. Новоселовой. М. : Проспект, 2019. С. 79.

¹⁴ Свидетельство о государственной регистрации программы для ЭВМ № 2015616907 // URL: <https://reestr.minsvyaz.ru/reestr/125769/> (дата обращения: 01.04.2019).

¹⁵ Договор ВОИС по авторскому праву (вместе с Согласованными заявлениями в отношении Договора ВОИС по авторскому праву) (подписан 20.12.1996) // СПС «КонсультантПлюс».

¹⁶ Савельев А. И. Правовая природа виртуальных объектов, приобретаемых за реальные деньги в многопользовательских играх // Вестник гражданского права. 2014. № 1. С. 127—150.

создавать собственные фильтры для данной платформы. Полагаем возможным применение механизмов авторско-правовой охраны по отношению к продуктам использования технологий виртуальной и дополненной реальности, если такие объекты обладают критериями охраноспособности (созданы творческим трудом, оригинальные, неповторимые, выраженные в объективной форме).

Одним из нарушений в данной сфере является копирование и перенос реальных объектов в виртуальную/дополненную среду¹⁷. Рассматриваемые технологии позволяют пользователям создать точную копию объекта, однако может ли при этом у пользователя возникнуть авторское право на данный объект? В зарубежной литературе отмечается, что создание точной копии объекта в виртуальной или дополненной реальности не может обеспечить охрану авторских прав, поскольку речь идет о недостаточном соблюдении условия о наличии творческого труда¹⁸. Более того, в случае копирования нередко возникает угроза нарушения чужих авторских прав.

Возникают также вопросы, связанные с защитой прав на производные произведения (ст. 1260 ГК РФ). Речь идет о тех случаях, когда пользователь объединяет чужую работу со своей (либо с другой), чтобы создать новое произведение. Например, пользователи дополненной реальности могут поместить виртуальный объект на существующее в реальной действительности произведение скульптуры; визуально объединить охраняемое авторским правом произведение, которое отображается в их смартфоне или очках, с фактической работой, которая появляется пе-

ред ними; использовать фильтры, которые изменяют внешний вид авторских произведений. Вопрос о квалификации таких объектов в качестве охраняемых авторским правом произведений остается открытым, однако подобные действия в некоторых случаях однозначно могут быть признаны нарушением исключительного права¹⁹.

Рассмотренное многообразие объектов, задействованных в теологиях виртуальной и дополненной реальности, позволяют сделать однозначный вывод о возможности реализации их охраны с помощью института авторских прав. Тем не менее творческая природа некоторых продуктов использования в виртуальной и дополненной реальности остается спорной ввиду отсутствия достаточного уровня творчества при их создании.

Патентно-правовые модели правовой охраны. Увеличение количества поданных заявок на патенты в последние годы свидетельствует как о темпах развития данных технологий, так и о стремлении заинтересованных сторон сохранить конкурентные преимущества путем обеспечения охраны своих изобретений. Наибольшая количество поданных заявок на патенты приходится на Северную Америку и Китай, также заявки подаются в Европе, Азии, Южной Америке и Австралии²⁰.

Основным объектом патентных прав, используемым в технологиях виртуальной и дополненной реальности, является изобретение (ст. 1350 ГК РФ). Примерами подобных технических решений могут послужить системы и методы для получения изображений виртуальной и дополненной реальности²¹, устройство для обеспечения симуляции предметов одежды²² и др.

¹⁷ Lemley M. A., Volokh E. Law, Virtual Reality, and Augmented Reality // University of Pennsylvania Law Review. April 2018. Vol. 166. No. 5. P. 1112.

¹⁸ См.: Afoaku M. The Reality of Augmented Reality and Copyright Law // Northwestern Journal of Technology and Intellectual Property. 2017. Vol. 15. P. 118.

¹⁹ Lemley M. A., Volokh E. Op. cit. P. 1112.

²⁰ Augmented and virtual reality: emerging legal implications of the «final platform» // Reed Smith LLP. URL: <https://www.reedsmith.com/-/media/files/perspectives/2017/06/augmented-virtual-reality-emerging-legal-implications-of-final-platform.pdf> (дата обращения: 01.04.2019).

²¹ US Patent No. 9,690,375 // URL: <https://patents.google.com/patent/US9690375B2/en> (дата обращения: 01.04.2019).

²² US Patent No. 8,275,590 // URL: <https://patents.google.com/patent/US8275590B2/en> (дата обращения: 01.04.2019).

В аналитическом материале, разработанном Всемирной организацией интеллектуальной собственности (ВОИС), указывается на следующие наиболее популярные направления изобретений в данной области: 3D-моделирование, обработка данных, устройства отображения, обработка данных изображений, устройства интерфейса и устройства обработки. В перспективе ожидается активная разработка изобретений с помощью технологий виртуальной и дополненной реальности в области медицины, спорта, архитектуры и обеспечения безопасности данных²³.

Важно отметить, что некоторые юрисдикции допускают регистрацию программного обеспечения при условии, что оно неразрывно связано с контролируемым им устройством. Так, в ст. 52 Европейской патентной конвенции прямо указывается на невозможность патентной охраны программного обеспечения, если оно не служит для управления технического устройства, заявленного в качестве изобретения²⁴. В США аналогичным образом судебная практика выработала тест (machine-or-transformation), позволяющий определить патентоспособность программ для ЭВМ. Суть данного теста заключается в том, что патент на программу может быть выдан только в случае, если она связана с определенным устройством либо с ее помощью происходит трансформация объекта в другое состояние²⁵. В этой связи в качестве изобретений в области виртуальной и дополненной реальности может выступать как аппаратное, так и программное обеспечение.

Немаловажное значение в развитии индустрии технологий виртуальной и дополненной реальности имеют дизайнерские решения. В качестве промышленных образцов

(ст. 1352 ГК РФ) могут выступать результаты художественного конструирования технических устройств, дизайн отображающихся на экране значков, интерфейс программы. Следует отметить, что, как и для моделей авторско-правовой охраны, при реализации патентно-правовой охраны результатов творческого труда, созданных в виртуальной и дополненной реальности, в настоящий момент применяются классические механизмы, характерные для объектов патентных прав.

Безусловно, основными институтами, обеспечивающими охрану технологий виртуальной и дополненной реальности, являются авторское и патентное право. Однако важной составляющей любого продукта является его узнаваемость среди потребителей. Данную функцию чаще всего обеспечивают товарные знаки (ст. 1477 ГК РФ). Предлагается также выделить *модель охраны с применением норм о средствах индивидуализации*.

Основным вопросом в данной области является возможность регистрировать товарные знаки для их использования непосредственно в виртуальном мире. В действительности использование товарных знаков и иных средств индивидуализации в виртуальной среде не редкость. Как правило, речь идет об использовании товарных знаков в играх и симуляторах. Зачастую разработчики и издатели мультимедийных продуктов регистрируют товарные знаки для дальнейшего использования как в реальной, так и в виртуальной среде²⁶. Однако может ли пользователь подобной платформы зарегистрировать товарный знак с целью его использования в виртуальной среде? Практика показывает, что подобные действия возможны. Например, в 2007 г. пользователь виртуального мира по-

²³ Virtual Reality: Patent Landscape Analysis // https://www.wipo.int/edocs/plrdocs/en/lexinnova_plr_virtual_reality.pdf (дата обращения: 01.04.2019).

²⁴ Конвенция о выдаче европейских патентов (Европейская патентная конвенция) от 05.10.1973 // URL: <http://docs.cntd.ru/document/902308644> (дата обращения: 05.04.2019).

²⁵ Чурилов А. Режимы охраны программ для ЭВМ: изобретение, коммерческая тайна или литературное произведение? // ИС. Авторское право и смежные права. 2017. № 7. С. 35—44.

²⁶ См., например: US Trademark No. 86588525 // URL: <http://tmsearch.uspto.gov/bin/showfield?f=doc&state=4801:agkxwn.3.9> (дата обращения: 05.04.2019).

лучил свидетельство на товарный знак в виде своего аватара²⁷. Вынуждены признать, однако, что подобные случаи весьма редки.

Несомненно, регистрация товарного знака для использования в виртуальной цифровой среде возможна только в случае коммерческого использования данного знака. Подобное можно сказать и о виртуальных товарных знаках, являющихся продуктами использования технологии дополненной реальности (нетрадиционные товарные знаки). Из всего этого следует, что институт товарных знаков может применяться в целях обеспечения охраны технологий виртуальной и дополненной реальности, а также продуктов их использования.

Широкое многообразие создания и исполнения результатов интеллектуальной деятельности в сфере технологий виртуальной и дополненной реальности выявляет проблемы обеспечения их правовой охраны. Вместе с тем следует отметить, что рассмотренные выше примеры свидетельствуют о том, что в настоящее время, благодаря действующим механизмам правовой охраны интеллектуальных прав, можно обеспечить охрану результатов интеллектуальной деятельности, создаваемых в виртуальной и дополненной реальности, но требуется дополнительное изучение и выработка новых моделей по охране результатов творческого труда в рассматриваемой сфере.

БИБЛИОГРАФИЯ

1. *Гринь Е. С.* Ты — автор. Что такое авторские и смежные права / под ред. Л. А. Новоселовой. — М. : Проспект, 2019. — 96 с.
2. *Гришкун А. В.* Терминологические особенности изучения технологии дополненной реальности при обучении информатике // Вестник Московского городского педагогического университета. Серия : Информатика и информатизация образования». — 2016. — № 4 (38). — С. 93—100.
3. *Иванов Д. В.* Виртуализация общества. — СПб., 2002. — 96 с.
4. *Кастельс М.* Информационная эпоха: экономика, общество и культура. — М., 2000. — 606 с.
5. *Кирик Т. А.* Виртуальная реальность: сущность, критерии, типология : дис. ... канд. филос. наук. — Омск, 2004.
6. *Носов Н. А.* Виртуальная реальность // Вопросы философии. — 1999. — № 10. — С. 152—164.
7. *Савельев А. И.* Правовая природа виртуальных объектов, приобретаемых за реальные деньги в многопользовательских играх // Вестник гражданского права. — 2014. — № 1. — С. 127—150.
8. *Таратута Е. Е.* Философия виртуальной реальности. — СПб., 2007. — 147 с.
9. *Федосеева Н. Н.* Виртуальное пространство — новая сфера функционирования современного государства (теоретический аспект) // Информационное право. — 2008. — № 3.
10. *Чурилов А.* Режимы охраны программ для ЭВМ: изобретение, коммерческая тайна или литературное произведение? // ИС. Авторское право и смежные права. — 2017. — № 7. — С. 35—44.
11. *Яковлев Б. С., Пустов С. И.* История, особенности и перспективы технологии дополненной реальности // Известия ТулГУ. Технические науки. — 2013. — № 3. — С. 479—484.
12. *Afoaku M.*, The Reality of Augmented Reality and Copyright Law // Northwestern Journal of Technology and Intellectual Property. — 2017. — Vol. 15. — Pp. 111—128.
13. *Azuma R. T.* A Survey of Augmented Reality // In Presence: Teleoperators and Virtual Environments. — 1997. — № 4. — Pp. 355—385.
14. *Lemley M. A., Volokh E.* Law, Virtual Reality, and Augmented Reality // University of Pennsylvania Law Abstract. — April 2018. — Vol. 166. — No. 5. — Pp. 1051—1138.

Материал поступил в редакцию 6 мая 2019 г.

²⁷ US Trademark No. 77110299 // URL: http://tsdr.uspto.gov/#caseNumber=77110299&caseType=SERIAL_NO&searchType=statusSearch (дата обращения: 05.04.2019).

FORMATION OF BASIC MODELS OF PROTECTION OF TECHNOLOGIES OF VIRTUAL AND AUGMENTED REALITY IN THE CONTEXT OF INTELLECTUAL PROPERTY RIGHTS²⁸

GRIN Elena Sergeevna, PhD in Law, Associate Professor, Deputy Head of the Department of Intellectual Rights of the Kutafin Moscow State Law University (MSAL)
esgrin@msal.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

KOROLEVA Anastasia Georgievna, Master's Student of the Department of Intellectual Rights of the Kutafin Moscow State Law University (MSAL)
agkoroleva@msal.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

Abstract. *Digital technologies development has affected almost all spheres of human activity. Today, technologies of virtual and augmented reality can be referred to as the most significant results of digital transformation of the economy. The qualitative development of these technologies, as well as their active and widespread application, leads to many legal problems. One of them involves the problems concerning determination of mechanisms of protection of technologies of virtual and augmented reality, as well as products of their use under the rules of intellectual property law. The article considers peculiarities of the legal nature of virtual and augmented reality technologies, analyzes the concepts of virtuality, virtual and augmented reality in the context of various approaches found in the relevant literature. The paper scrutinizes the main objects of intellectual rights implemented in technologies of virtual and augmented reality, as well as objects generated by them. The authors draw a conclusion that it is possible to ensure protection of the results of intellectual activity and means of individualization by the main institutions of intellectual property rights protection, but the authors express concerns about the need to develop new models to protect the results of creative work in this area.*

Keywords: *intellectual rights, virtual reality, new technologies, intellectual property, copyright, author, results of intellectual activity, augmented reality, right holder, commercialization, digital technologies.*

REFERENCES (TRANSLITERATION)

1. Grin' E. S. Ty — avtor. Chto takoe avtorskie i smezhnye prava / pod red. L. A. Novoselovoj. — M. : Prospekt, 2019. — 96 s.
2. Grishkun A. V. Terminologicheskie osobennosti izucheniya tekhnologii dopolnennoj real'nosti pri obuchenii informatike // Vestnik Moskovskogo gorodskogo pedagogicheskogo universiteta. Seriya : Informatika i informatizaciya obrazovaniya». — 2016. — № 4 (38). — S. 93—100.
3. Ivanov D. V. Virtualizaciya obshchestva. — SPb., 2002. — 96 s.
4. Kastel's M. Informacionnaya epoha: ekonomika, obshchestvo i kul'tura. — M., 2000. — 606 s.
5. Kirik T. A. Virtual'naya real'nost': sushchnost', kriterii, tipologiya : dis. ... kand. filos. nauk. — Omsk, 2004.
6. Nosov N. A. Virtual'naya real'nost' // Voprosy filosofii. — 1999. — № 10. — S. 152—164.
7. Savel'ev A. I. Pravovaya priroda virtual'nyh ob'ektov, priobretaemyh za real'nye den'gi v mnogopol'zovatel'skih igrakh // Vestnik grazhdanskogo prava. — 2014. — № 1. — S. 127—150.
8. Taratuta E. E. Filosofiya virtual'noj real'nosti. — SPb., 2007. — 147 s.
9. Fedoseeva N. N. Virtual'noe prostranstvo — novaya sfera funkcionirovaniya sovremennogo gosudarstva (teoreticheskij aspekt) // Informacionnoe pravo. — 2008. — № 3.
10. Churilov A. Rezhimy ohrany programm dlya EVM: izobretenie, kommercheskaya tajna ili literaturnoe proizvedenie? // IS. Avtorskoe pravo i smezhnye prava. — 2017. — № 7. — S. 35—44.
11. Yakovlev B. S., Pustov S. I. Istoriya, osobennosti i perspektivy tekhnologii dopolnennoj real'nosti // Izvestiya TulGu. Tekhnicheskie nauki. — 2013. — № 3. — S. 479—484.

²⁸ The study was carried out with the financial support of the RFBR No. 18-29-16199 MK «The Concept of Intellectual Rights in the Field of Virtual and Augmented Reality Technologies.»

ТРУДОВЫЕ ОТНОШЕНИЯ И СОЦИАЛЬНОЕ ОБЕСПЕЧЕНИЕ

Н. Л. Лютов*

Адаптация трудового права к развитию цифровых технологий: вызовы и перспективы¹

***Аннотация.** В статье анализируются два ключевых вызова для трудового права, возникших в связи с развитием информационных технологий: изменение структуры занятости (переход трудовой деятельности из сферы производства в сферу услуг, отмирание старых и появление новых профессий) и трансформация трудового отношения в связи с возникновением новых форм занятости, приводящая к эрозии важнейших признаков трудового отношения, включая подчинение работника работодателю и контроль за осуществлением труда как процесса. В связи с первым вызовом автор рассматривает проблемы регулирования труда наиболее уязвимой с точки зрения изменения видов профессий категории работников — работников пенсионного и предпенсионного возраста.*

По второму вызову автор предлагает обсудить возможности защиты трудовых прав работающих в случае экономической зависимости лица, выполняющего работу, от лица, которое поручает выполнить эту работу, независимо от формы договора, заключенного между сторонами.

***Ключевые слова:** трудовое отношение, трансформация труда, новые формы занятости, трудовой договор, нетипичная занятость, цифровая экономика, неустойчивая занятость, пожилые работники.*

DOI: 10.17803/1994-1471.2019.103.6.098-107

В 2019 г. Международная организация труда (МОТ) отмечает свое столетие. МОТ была учреждена в 1919 г. в качестве ответа на крупнейшие социальные катаклизмы, потрясшие общество в эпоху промышленной революции. Через 100 лет после учреждения МОТ международное и национальное право

большинства стран мира также сталкивается с серьезнейшими вызовами, связанными с необходимостью переосмысления его фундаментальных основ.

И так же, как и 100 лет назад, вызовы в сфере труда тесно связаны с научно-техническим прогрессом. Промышленная революция

¹ Публикация подготовлена в рамках поддержанного РФФИ научного проекта № 18-29-16126.

© Лютов Н. Л., 2019

* Лютов Никита Леонидович, доктор юридических наук, профессор, заведующий кафедрой трудового права и права социального обеспечения Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)

nlljutov@msal.ru

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

XVIII—XIX в. стала причиной формирования основ трудового права в его классическом виде, включая концепцию трудового договора, имеющего отличную от гражданско-правовых договоров природу, регулирование важнейших институтов трудового права, таких как рабочее время и время отдыха, оплата труда, безопасность и гигиена труда и др. В ходе промышленной революции сформировалось и профсоюзное движение, которое заставило стороны социального диалога выстроить модели коллективного трудового права.

Начало XXI в. характеризуется так называемой четвертой промышленной революцией, или цифровизацией экономики и социальных отношений. Переход экономики из индустриальной стадии развития в постиндустриальную оказывает определяющее влияние на отношения между работниками и работодателями. Неслучайно поэтому, что как в МОТ, так и в среде научных исследователей по трудовому праву, экономике и социологии труда в последнее время все чаще поднимаются вопросы о том, как именно изменится регламентация отношений в сфере труда в XXI в. Этому вопросу посвящен и известный доклад генерального директора Международного бюро труда 2015 г. «Будущее сферы труда»², и вышедший в начале 2019 г. доклад Глобальной комиссии по вопросам будущего сферы труда³, и большое количество научных публикаций. В рамках Европейского Союза в настоящее время обсуждается принятие новой большой рамочной Директивы ЕС, связанной с воздействием информационных технологий на рынок труда и с трансформацией трудовых отношений, под рабочим названием «О прозрачных и предсказуемых условиях труда в Европейском Союзе»⁴. К сожалению или к сча-

стью, но Россия и евразийское пространство тоже не остались в изоляции от этих мировых тенденций.

В чем же конкретно состоят вызовы для рынка труда и трудовых отношений в связи с информационной технологической революцией начала XXI в.?

ВЫЗОВ ПЕРВЫЙ: ОТОМРЕТ ЛИ ЧЕЛОВЕЧЕСКИЙ ТРУД?

Строго говоря, ничего принципиально нового в этом вызове нет. Само трудовое право зародилось как ответ на тот же самый вызов, поставленный промышленной революцией в XVIII—XIX вв. Промышленная революция выразилась в технологическом усовершенствовании производственного оборудования, позволившем начать массовое промышленное производство продукции и высвободившем рабочую силу, ранее занятую более примитивным производством. В результате возник резкий дисбаланс на рынке труда, сильнейший перекос спроса и предложения труда в сторону предложения и, как следствие, навязывание работодателями кабальных условий труда работникам. Огромная продолжительность рабочего времени, мизерная оплата труда, обман работодателями работников при расчете, массовое использование детского труда — все это стало следствием технологического прогресса, приведшего к потере старых рабочих мест очень значительной части населения в странах — пионерах промышленной революции.

Ограничение свободы договора в сфере труда законодательными нормами с целью защиты экономически более слабой стороны — работника, признание того факта, что труд, выполня-

² Международная конференция труда, 104-я сессия, 2015 г. Доклад Генерального директора МБТ «Инициатива столетия, касающаяся будущего сферы труда». Женева : МБТ, 2015.

³ Работать ради лучшего будущего / Глобальная комиссия по вопросам будущего сферы труда ; Международное бюро труда. Женева : МБТ, 2019. URL: https://www.ilo.org/wcmsp5/groups/public/---dgreports/--cabinet/documents/publication/wcms_662472.pdf.

⁴ European Commission. Proposal for a Directive of the European Parliament and of the Council on transparent and predictable working conditions in the European Union. Brussels, 21.12.2017 COM(2017) 797 final 2017/0355(COD). URL: <https://eur-lex.europa.eu/legal-content/en/TXT/HTML/?uri=CELEX:52017PC0797&from=EN>.

емый под контролем работодателя, неотделим от личности работника и, следовательно, не может считаться товаром, признание права на объединение в профсоюзы, до этого считавшиеся преступным сговором, направленным на ограничение свободы торговли (трудом), — все это стало следствием первой промышленной революции.

Еще в промышленную эру, в середине XX в., не только футурологи и ученые, но и журналисты и писатели высказывали опасения по поводу того, что автоматизация производства вскоре вытеснит человека из сферы труда и подавляющее большинство населения окажется ненужным. К примеру, роман Курта Воннегута «Механическое пианино», впервые изданный еще в 1952 г., описывает антиутопию, в которой бесчеловечные механизированные алгоритмы отбирают наиболее технически одаренных людей, позволяя им попасть в привилегированную касту инженеров, а подавляющее большинство населения никому не нужно и направляется либо на дорожные работы, либо в армию, просто чтобы получить хоть какое-то занятие.

В начале XXI в. мы видим, что антиутопия середины XX в. не реализовалась. Однако опасения по поводу той же самой угрозы остались, и необходимо признать, что у этих опасений есть некоторые основания. В результате масштабного включения в человеческую жизнь информационных и телекоммуникационных технологий стало происходить массовое отмирание устаревающих профессий, сопровождаемое возникновением новых видов труда, направленных на обслуживание нового технологического уклада. Несмотря на опасения, что люди будут

вскоре заменены роботами, оптимистический взгляд на этот процесс исходит из того, что новые профессии вовлекут большее количество людей, чем число тех, кто потеряет работу из-за технологической революции⁵.

Даже если будет реализовываться этот оптимистичный сценарий, смена структуры занятости не будет безболезненной: терять работу будут преимущественно работники старшего возраста, а получать новые технологичные рабочие места будет в основном молодежь. Согласно некоторым исследованиям, в ближайшее время в мире уйдет в прошлое или будет коренным образом трансформировано более половины нынешних видов трудовой деятельности⁶. И если молодые люди относительно легко могут адаптироваться к изменениям в мире труда, то старшему поколению такая адаптация дастся очень сложно. Существенная часть пожилых работников и даже работников старшего среднего возраста, теряя «традиционную» работу, уже не сможет найти занятость на «обновленном» рынке труда.

К сожалению, приходится констатировать, что политика нашего государства в сфере правовой регламентации труда не учитывает эту тенденцию. Повышение пенсионного возраста вынуждает пожилых работников держаться за свои рабочие места так долго, насколько они физически могут. С учетом того что приспособиться к новым профессиональным требованиям и новым профессиям пожилым работникам значительно труднее, работодатели стремятся и будут стремиться омолодить свой кадровый состав. Введенная в октябре 2018 г. новая статья 144.1 Уголовного кодекса Российской Федера-

⁵ См. об этом: Международная конференция труда, 104-я сессия, 2015 г. Доклад Генерального директора МБТ «Инициатива столетия, касающаяся будущего сферы труда». С. 12.

⁶ Berger R. The Industrie 4.0 transition quantified. Munich, 2016 // URL: https://www.rolandberger.com/de/Publications/pub_the_industrie_4_0_transition_quantified.htm ; Chang J.-H., Huynh P. ASEAN in transformation — The future of jobs at risk of automation // Bureau for Employers' Activities. Working Paper No. 9. Bangkok : ILO Regional Office for Asia and the Pacific, 2016. URL: http://ilo.org/public/english/dialogue/actemp/downloads/publications/2016/asean_in_transf_2016_r2_future.pdf ; Frey C. B., Osborne M. The future of employment: How susceptible are jobs to computerisation? // Oxford Martin School Working Paper. Oxford, 2013. URL: <http://www.oxfordmartin.ox.ac.uk/publications/view/1314> ; PricewaterhouseCoopers. The long-view: How will the global economic order change by 2050? London, 2017 // URL: <https://www.pwc.com/gx/en/world-2050/assets/pwc-world-in-2050-summary-report-feb-2017.pdf>.

ции⁷, предусматривающая уголовную ответственность за необоснованный отказ в приеме на работу или необоснованное увольнение лица, достигшего предпенсионного возраста, не только не поможет предотвратить дискриминацию работников пенсионного и предпенсионного возраста, а скорее сыграет негативную роль. Она не повысит уровень защиты таких работников, поскольку необходимое условие ее применения — доказывание мотива преступления, т.е. достижения работником определенного возраста. Практика применения иной нормы, схожей по смыслу и содержанию, но касающейся беременных женщин и женщин с детьми до трех лет (ст. 145 УК РФ), показывает, что этот мотив практически недоказуем. При этом сам факт включения этой нормы в УК РФ будет психологически мотивировать работодателей избегать пожилых работников всеми способами.

В ТК РФ есть противоречивая норма противоположной направленности: ст. 59 позволяет заключать срочный трудовой договор с работниками, достигшими пенсионного возраста. С одной стороны, эта норма снижает уровень защиты от увольнения этой категории работников, и в связи с этим она рассматривалась Конституционным Судом на предмет противоречия Конституции РФ⁸. С другой стороны, право работодателя и работников заключать в этой ситуации срочные трудовые договоры повышает привлекательность пожилых работников для работодателей, понимающих, что срочный трудовой договор — это инструмент, с помощью которого они смогут избавиться от работника с минимальными рисками, особенно с учетом упомянутой неудачной законодательной новации осени 2018 г.

Приходится констатировать, что пока российское трудовое законодательство не дает адекватных ответов на вызовы, связанные с изменением профессиональной структуры рынка труда и особыми проблемами, возникающими в связи с этим у пожилых работников.

ВЫЗОВ ВТОРОЙ: ТРАНСФОРМАЦИЯ ТРУДА И ТРУДОВЫХ ОТНОШЕНИЙ

Технологическая революция оказывает мощнейшее влияние не только на количественные, но и на качественные характеристики занятости. С этой точки зрения важно не только то, что отдельные профессии уходят в прошлое, а новые возникают, но и тот факт, что традиционные подходы к трудовому правоотношению становятся все менее применимы. Это заметно даже по текстуальному объему трудового законодательства. Трудовой кодекс РФ стал первым отечественным кодифицированным актом о труде, включившим отдельную часть, касающуюся отдельных категорий работников, т.е. массу специальных правовых норм, предусматривающих особенности правового регулирования трудовых правоотношений, не укладывающихся в общие рамки. При этом с момента вступления в силу в 2002 г. по настоящее время объем ТК РФ увеличился почти в два раза, по большей части за счет включения новых специальных норм, посвященных отдельным, нетипичным трудовым отношениям. Становится актуальным вопрос: насколько общее понятие трудового отношения (ст. 15 ТК РФ) и трудового договора (ст. 56 ТК РФ) продолжают соответствовать практике регулирования труда?⁹

⁷ См.: Федеральный закон от 03.10.2018 № 352-ФЗ // СЗ РФ. 2018. № 41. Ст. 6192.

⁸ Определение Конституционного Суда РФ от 15.05.2007 № 378-О-П «Об отказе в принятии к рассмотрению запроса Амурского городского суда Хабаровского края о проверке конституционности положения статьи 59 Трудового кодекса Российской Федерации» // Вестник Конституционного Суда РФ. 2007. № 6.

⁹ См. об этом, например: Головина С. Ю. Современные тенденции в трудовом праве России // Современные тенденции в развитии трудового права и права социального обеспечения : материалы Междунар. научн.-практ. конференции (Москва, 18—20 января 2006 г.) / под ред. К. Н. Гусова. М. : Проспект, 2007. С. 9—22 ; Нуртдинова А. Ф., Чиканова Л. А. Дифференциация регулирования трудовых отношений как закономерность развития трудового права // Журнал российского права. 2015. № 6. С. 68—82 ; Орловский Ю. П. Единство и дифференциация трудового законодательства // Право человека на жизнь

Тенденция роста дифференциации в правовом регулировании труда характерна не только для России, но и для зарубежных стран. Так, например, в отношении Германии высказывается мнение о том, что корректнее уже говорить не об увеличении масштаба нестандартной занятости, а о том, что само трудовое правоотношение приобретает новые черты и не все классические критерии трудового отношения для этого «нового стандартного трудового отношения» применимы в полной степени¹⁰.

Рост дифференциации труда и феномен нестандартной занятости связан с тем, что трудовое право в его нынешнем виде выкристаллизовалось в эпоху промышленной революции. Именно исходя из необходимости защиты фабричных рабочих, выполняющих однотипные операции под контролем работодателя, сформировались ключевые институты современного трудового права. Для регламентации субординированного и контролируемого работодателем труда очень подходят такие институты трудового права, как рабочее время и время отдыха, оплата труда, безопасность и гигиена труда и др. Современный труд, опосредован-

ный информационными технологиями и чаще всего относящийся к сфере услуг, гораздо более самостоятелен по своему характеру с точки зрения того, как именно выполняется работа. При этом занятые в выполнении такого труда люди нуждаются в защите в не меньшей степени, чем фабричные рабочие.

Понимание трудового правоотношения как несамостоятельного, субординированного труда¹¹, либо, в соответствии с отечественной правовой традицией, как отношения, отличающегося от гражданско-правового по личностному, организационному и имущественному признакам¹², становится применимым ко все меньшему числу сфер трудовой деятельности.

В 2015 г. Европейский фонд по улучшению условий труда и жизни (Еврофонд) опубликовал масштабный обзор, в котором анализируются «новые формы занятости» в Европе¹³.

В этом исследовании к новым формам занятости относят *совместное использование труда работников*, в рамках которого группа работодателей одновременно нанимает работников и солидарно либо субсидиарно отвечает перед работниками; *совместное трудоустройство*

и гарантии его реализации в сфере труда и социального обеспечения : материалы научно-практической конференции / под ред. К. Н. Гусова. М., 2008. С. 27—30 ; Проблемы дифференциации в правовом регулировании отношений в сфере труда и социального обеспечения : материалы науч.-практ. конференции / под ред. К. Н. Гусова. М., 2009. 544 с.

¹⁰ International Labour Organization. Synthesis Report of the National Dialogues on the Future of Work. Geneva : International Labour Office, 2017. P. 38.

¹¹ См.: *Bercusson B.* Employment Protection // *Labour Law and Social Europe: Selected writings of Brian Bercusson*. Brussels : European Trade Union Institute, 2009. Pp. 241—306 ; *Freedland M.* The Personal Employment Contract. Oxford : Oxford University Press, 2006. Pp. 26—35 ; *Restatement of Labour Law in Europe / B. Waas, G. H. van Voss (eds.)*. Oxford and Portland : Hart Publishing, 2017. Vol. I : The Concept of Employee. 806 p. ; *Supiot A.* Beyond Employment: Changes in Work and the Future of Labour Law in Europe. Oxford : Oxford University Press, 2001. Pp. 10—17 et al.

¹² См. об этом, например: *Бугров Л. Ю.* Трудовой договор в России и за рубежом. Пермь : Перм. гос. нац. ун-т, 2013. С. 29—66 ; *Гусов К. Н., Толкунова В. Н.* Трудовой договор. М., 1996 ; *Дивеева Н. В.* Теоретические проблемы индивидуального правового регулирования трудовых отношений : дис. ... д-ра юрид. наук. СПб., 2008. 396 с. ; Курс российского трудового права / под ред. Е. Б. Хохлова. СПб. : Изд-во Р. Асланова «Юридический центр-Пресс», 2007. Т. 3 : Трудовой договор. С. 87—116 ; *Тарусина Н. Н., Лушников А. М., Лушников М. В.* Социальные договоры в праве : монография. М. : Проспект, 2017. С. 191—270 ; *Томашевский К. Л.* Определение трудового отношения: от доктринальных разработок к легальному закреплению в государствах — членах ЕАЭС // Трудовое право в России и за рубежом. 2018. № 1. С. 3—6.

¹³ Eurofound. New forms of employment. Luxembourg : Publications Office of the European Union, 2015. 168 p. URL: https://www.eurofound.europa.eu/sites/default/files/ef_publication/field_ef_document/ef1461en.pdf.

означает противоположный тип отношений, при котором один работодатель заключает трудовой договор сразу с несколькими работниками для коллективного выполнения одной работы; *краудворкинг*, *краудсорсинг* — при которых связь между исполнителем и заказчиком осуществляется через посредничество онлайн-платформы¹⁴; *мобильная работа, основанная на информационно-коммуникационных технологиях*, — форма трудовых отношений, обозначенная в ТК РФ как дистанционный труд.

Наибольшую тревогу вызывает рост так называемой *разовой работы* (англ. — casual work) и *договоров с нулевым рабочим временем* (англ. — zero-hours contracts), в рамках которых работодатель не обязан предоставлять работу работнику даже в минимальном объеме, но при этом может вызывать работника тогда, когда это ему нужно и удобно. Работник при таких схемах трудовых отношений вынужден надеяться, что его вызовут и дадут какой-то объем работы без каких-либо гарантий, но при этом он формально не относится к безработным и не имеет права на получение пособия по безработице. Такие формы труда, лишаящие работника стабильности в трудовых отношениях и, чаще всего, важнейших трудовых гарантий, в настоящее время имеют тенденцию к существенному росту.

Это далеко не исчерпывающий перечень форм труда, относящихся к так называемой но-

вой занятости, однако объем статьи не позволяет говорить о них подробнее.

Применительно к нашей стране вызовы, связанные с видоизменением занятости и трудовых отношений, актуальны не меньше, чем для экономически развитых зарубежных стран. В связи с этим возникают сложности не только с технико-юридической адаптацией норм «традиционного» трудового права к новым формам труда и наоборот, но и, что более важно, с необходимостью выстраивания адекватной системы гарантий реализации трудовых прав людей, вовлеченных в новые формы занятости.

Не все, но многие из новых форм труда характеризуются как неустойчивая занятость (англ. — precarious employment)¹⁵. Неустойчивую занятость принято определять как вынужденную утрату работником стандартных трудовых отношений, основанных на трудовом договоре с неопределенным сроком и полным рабочим временем¹⁶. В настоящее время в странах с развитой рыночной экономикой масштабы неустойчивой занятости значительно увеличиваются¹⁷. Рост неустойчивости труда затронул и нашу страну¹⁸.

Представляется, что органам нашей законодательной и исполнительной власти следует обратить внимание не только и не столько на технические аспекты воздействия информационных технологий на трудовые отношения¹⁹,

¹⁴ См.: Green A., Barnes S.-A. CrowdEmploy. Part I: Crowdsourcing for paid work. An empirical investigation into the impact of crowdsourcing for paid work on employability. Warwick Institute for Employment Research/Institute for Prospective Technological Studies (IPTS), Warwick/Seville, 2013; Чесалина О. В. Работа на основе интернет-платформ (crowdwork и work on demand via apps) как вызов трудовому и социальному праву // Трудовое право в России и за рубежом. 2017. № 1. С. 52—55.

¹⁵ Fudge J. The Legal Boundaries of the Employer, Precarious Workers, and Labour Protection // Boundaries and Frontiers of Labour Law: Goals and Means in the Regulation of Work / G. Davidov, B. Langille (eds.). Oxford: Hart Publishing, 2006. P. 296.

¹⁶ См.: Неустойчивая занятость в Российской Федерации: теория и методология выявления, оценивание и вектор сокращения / под ред. В. Н. Бобкова. М.: Кнорус, 2018. С. 6—7.

¹⁷ Benach J., Vives A., Amable M., Vanroelen C., Tarafa G., Muntaner C. Precarious Employment: Understanding an Emerging Social Determinant of Health // Annual Review of Public Health. 2014. Vol. 35. Pp. 229—253. URL: <https://www.annualreviews.org/doi/full/10.1146/annurev-publhealth-032013-182500>.

¹⁸ См.: Голенкова З. Т., Голиусова Ю. В. Прекариат как новая группа наемных работников // Уровень жизни населения регионов России. 2015. № 1. С. 47—57.

¹⁹ О такого рода действиях государства см.: Костян И. А., Куренной А. М., Хныкин Г. В. Трудовое право и цифровая экономика: сочетаются ли они? // Трудовое право в России и за рубежом. 2017. № 4. С. 10—12.

в частности на электронное взаимодействие работника и работодателя, документооборот, электронные трудовые книжки и т.п., но и на более важную проблему роста неустойчивости трудовых отношений в ходе развития новых форм занятости. Для преодоления этой негативной тенденции следует принимать меры программного характера, основанные на научных исследованиях этой проблемы, осуществляемых юристами, социологами и экономистами.

Академическим же специалистам в области трудового права следует осмыслить и предложить обществу и государству новые подходы к понятию трудового отношения и трудовому договору, учитывающие смещение акцента с факта подчинения работника работодателю на факт экономической зависимости лица, выполняющего работу, без привязки к конкретной форме занятости.

ЗАКЛЮЧЕНИЕ

В этой статье затронуты лишь некоторые глобальные проблемы, связанные с воздействием информационных технологий на рынок труда и трудовое право. За рамками статьи остались другие, не менее важные аспекты этого явления, такие как глобальное ослабление традиционных механизмов представительства работников с помощью профсоюзов и связанное с этим изменение баланса сил сторон трудовых отношений в пользу работодателей. Кроме того, с технологической революцией связана

и глобализация мировой хозяйственной деятельности, также оказывающая серьезное и очень часто негативное воздействие на возможности защиты трудовых прав в результате конкуренции отдельных государств за привлечение иностранных инвесторов путем отказа от социальных стандартов, — так называемая «гонка на дно»²⁰.

Однако и рассмотренные в статье проблемы нуждаются не только в углубленном анализе на уровне научной доктрины, например в отношении переосмысления подходов к понятию трудового правоотношения, но и в конкретных действиях законодательной и исполнительной власти, направленных на минимизацию негативных аспектов технологического прогресса в части регулирования труда.

В частности, в связи с этим необходим пересмотр решения о повышении пенсионного возраста, пересмотр бессмысленных с точки зрения защиты трудовых прав и рассчитанных исключительно на медийный эффект норм о запрете отказа в заключении трудового договора и увольнения по инициативе работодателя работников старшего возраста. Более важно то, требуется разработка программных и масштабных мер, направленных на адаптацию работников старших поколений к меняющемуся миру труда (обучение новым профессиям, помощь в профессиональной ориентации и др.), налоговое стимулирование работодателей, принимающих на работы на профессии, недавно появившиеся на рынке труда, работников старшего возраста.

БИБЛИОГРАФИЯ

1. Бугров Л. Ю. Трудовой договор в России и за рубежом. — Пермь : Пермский государственный национальный университет, 2013. — 642 с.
2. Голенкова З. Т., Голицова Ю. В. Прекариат как новая группа наемных работников // Уровень жизни населения регионов России. — 2015. — № 1. — С. 47—57.

²⁰ См. об этом: *Люттов Н. Л.* Международные трудовые стандарты и международная торговля в условиях глобализации: проблемы взаимодействия (в свете вступления России в ВТО) // *Российский юридический журнал.* 2013. № 6 (93). С. 127—134; *Люттов Н. Л.* Всемирная торговая организация: перспективы участия в установлении международных трудовых стандартов // *Трудовое право.* 2009. № 7. С. 80—84.

3. Головина С. Ю. Современные тенденции в трудовом праве России // Современные тенденции в развитии трудового права и права социального обеспечения : материалы Междунар. научн.-практ. конф. (Москва, 18—20 января 2006 г.) / под ред. К. Н. Гусова. — М. : Проспект, 2007. — С. 9—22.
4. Гусов К. Н., Толкунова В. Н. Трудовой договор. — М., 1996. — 126 с.
5. Дивеева Н. В. Теоретические проблемы индивидуального правового регулирования трудовых отношений : дис. ... д-ра юрид. наук. — СПб., 2008. — 396 с.
6. Костян И. А., Куренной А. М., Хныкин Г. В. Трудовое право и цифровая экономика: сочетаются ли они? // Трудовое право в России и за рубежом. — 2017. — № 4. — С. 10—12.
7. Курс российского трудового права / под ред. Е. Б. Хохлова. — СПб. : Изд-во Р. Асланова «Юридический центр-Пресс», 2007. — Т. 3 : Трудовой договор. — 656 с.
8. Лютов Н. Л. Всемирная торговая организация: перспективы участия в установлении международных трудовых стандартов // Трудовое право. — 2009. — № 7. — С. 80—84.
9. Лютов Н. Л. Международные трудовые стандарты и международная торговля в условиях глобализации: проблемы взаимодействия (в свете вступления России в ВТО) // Российский юридический журнал. — 2013. — № 6 (93). — С. 127—134.
10. Международная конференция труда, 104-я сессия, 2015 г. Доклад Генерального директора МБТ «Инициатива столетия, касающаяся будущего сферы труда». — Женева : МБТ, 2015.
11. Неустойчивая занятость в Российской Федерации: теория и методология выявления, оценивание и вектор сокращения / под ред. В. Н. Бобкова. — М. : Кнорус, 2018. — 342 с.
12. Нуртдинова А. Ф., Чиканова Л. А. Дифференциация регулирования трудовых отношений как закономерность развития трудового права // Журнал российского права. — 2015. — № 6. — С. 68—82.
13. Орловский Ю. П. Единство и дифференциация трудового законодательства // Право человека на жизнь и гарантии его реализации в сфере труда и социального обеспечения : материалы научно-практической конференции / под ред. К. Н. Гусова. — М., 2008. — С. 27—30.
14. Проблемы дифференциации в правовом регулировании отношений в сфере труда и социального обеспечения : материалы научно-практической конференции / под ред. К. Н. Гусова. — М., 2009. — 544 с.
15. Работать ради лучшего будущего / Глобальная комиссия по вопросам будущего сферы труда : Международное бюро труда. — Женева : МБТ, 2019. — URL: https://www.ilo.org/wcmsp5/groups/public/-dgreports/-cabinet/documents/publication/wcms_662472.pdf.
16. Тарусина Н. Н., Лушников А. М., Лушникова М. В. Социальные договоры в праве : монография. — М. : Проспект, 2017. — 480 с.
17. Томашевский К. Л. Определение трудового отношения: от доктринальных разработок к легальному закреплению в государствах — членах ЕАЭС // Трудовое право в России и за рубежом. — 2018. — № 1. — С. 3—6.
18. Чесалина О. В. Работа на основе интернет-платформ (crowdwork и work on demand via apps) как вызов трудовому и социальному праву // Трудовое право в России и за рубежом. — 2017. — № 1. — С. 52—55.
19. Benach J., Vives A., Amable M., Vanroelen C., Tarafa G., Muntaner C. Precarious Employment: Understanding an Emerging Social Determinant of Health // Annual Review of Public Health. — 2014. — Vol. 35. — Pp. 229—253. — URL: <https://www.annualreviews.org/doi/full/10.1146/annurev-publhealth-032013-182500>.
20. Bercusson B. Employment Protection // Labour Law and Social Europe: Selected writings of Brian Bercusson. — Brussels : European Trade Union Institute, 2009. — Pp. 241—306.
21. Berger R. The Industrie 4.0 transition quantified. — Munich, 2016. — URL: https://www.rolandberger.com/de/Publications/pub_the_industrie_4_0_transition_quantified.htm.
22. Chang J.-H., Huynh P. ASEAN in transformation — The future of jobs at risk of automation // Bureau for Employers' Activities. Working Paper No. 9. — Bangkok : ILO Regional Office for Asia and the Pacific, 2016. — URL: http://ilo.org/public/english/dialogue/actemp/downloads/publications/2016/asean_in_transf_2016_r2_future.pdf.
23. Eurofound. New forms of employment. — Luxembourg : Publications Office of the European Union, 2015. — 168 p. — URL: https://www.eurofound.europa.eu/sites/default/files/ef_publication/field_ef_document/ef1461en.pdf.

24. European Commission. Proposal for a Directive of the European Parliament and of the Council on transparent and predictable working conditions in the European Union. Brussels, 21.12.2017 COM(2017) 797 final 2017/0355(COD). — URL: <https://eur-lex.europa.eu/legal-content/en/TXT/HTML/?uri=CELEX:52017PC0797&from=EN>.
25. *Freedland M.* The Personal Employment Contract. — Oxford : Oxford University Press, 2006. — 560 p.
26. *Frey C. B., Osborne M.* The future of employment: How susceptible are jobs to computerisation? // Oxford Martin School Working Paper. — Oxford, 2013. — URL: <http://www.oxfordmartin.ox.ac.uk/publications/view/1314>.
27. *Fudge J.* The Legal Boundaries of the Employer, Precarious Workers, and Labour Protection // Boundaries and Frontiers of Labour Law: Goals and Means in the Regulation of Work / G. Davidov, B. Langille (eds.). — Oxford : Hart Publishing, 2006. — Pp. 295—316.
28. International Labour Organization. Synthesis Report of the National Dialogues on the Future of Work. — Geneva : International Labour Office, 2017. — 78 p.
29. PricewaterhouseCoopers. The long-view: How will the global economic order change by 2050? — London, 2017. — URL: <https://www.pwc.com/gx/en/world-2050/assets/pwc-world-in-2050-summary-report-feb-2017.pdf>.
30. Restatement of Labour Law in Europe / B. Waas, G.H. van Voss (eds.). — Oxford and Portland : Hart Publishing, 2017. — Vol. I : The Concept of Employee. — 806 p.
31. *Supiot A.* Beyond Employment: Changes in Work and the Future of Labour Law in Europe. — Oxford : Oxford University Press, 2001. — 246 p.

Материал поступил в редакцию 6 мая 2019 г

LABOUR LAW ADAPTATION TO THE DIGITAL TECHNOLOGIES: CHALLENGES AND PERSPECTIVES²¹

LYUTOV Nikita Leonidovich, Doctor of Law, Professor, Head of the Department of Labor and Social Security Law of the Kutafin Moscow State Law University (MSAL)
nlljutov@msal.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

Abstract. *The article deals with two key challenges to the labour law associated with the digital technologies' development: changing structure of employment in general (the shift of economy from industrial production to services' model, emergence of the new professions accompanied with decline of the traditional ones, etc.) and transformation of employment relations because of the growing number of new types of work. The latter trend leads to the problem of erosion of the key traditional features of employment relations including the subordination and control by the employer.*

In the light of the first challenge, the author considers the issues of the most vulnerable group of workers — employees of the pensionary and pre-pensionary age.

The second issue of transformation of employment leads the author to the proposal to start the academic debate concerning the perspectives of establishment of legal mechanisms of the economically dependent workers irrespective of their legal status (employment or civil law relations).

Keywords: *employment relations, employment contract, atypical employment, digital economy, precarious employment, senior workers.*

²¹ The publication is prepared with the financial support of the Russian Foundation for Basic Research, Research Project No. 18-29-16126.

REFERENCES (TRANSLITERATION)

1. Bugrov L. Yu. *Trudovoj dogovor v Rossii i za rubezhom.* — Perm' : Permskij gosudarstvennyj nacional'nyj universitet, 2013. — 642 s.
2. Golenkova Z. T., Goliusova Yu. V. *Prekariat kak novaya gruppa naemnyh rabotnikov // Uroven' zhizni naseleniya regionov Rossii.* — 2015. — № 1. — S. 47—57.
3. Golovina S. Yu. *Sovremennye tendencii v trudovom prave Rossii // Sovremennye tendencii v razvitii trudovogo prava i prava social'nogo obespecheniya : materialy Mezhdunar. nauchn.-prakt. konf. (Moskva, 18—20 yanvarya 2006 g.) / pod red. K. N. Gusova.* — M. : Prospekt, 2007. — S. 9—22.
4. Gusov K. N., Tolkunova V. N. *Trudovoj dogovor.* — M., 1996. — 126 s.
5. Diveeva N. V. *Teoreticheskie problemy individual'nogo pravovogo regulirovaniya trudovyh otnoshenij : dis. ... d-ra jurid. nauk.* — SPb., 2008. — 396 s.
6. Kostyan I. A., Kurennoj A. M., Hnykin G. V. *Trudovoe pravo i cifrovaya ekonomika: sochetayutsya li oni? // Trudovoe pravo v Rossii i za rubezhom.* — 2017. — № 4. — S. 10—12.
7. *Kurs rossijskogo trudovogo prava / pod red. E. B. Hohlova.* — SPb. : Izd-vo R. Aslanova «Yuridicheskij centr-Press», 2007. — T. 3 : *Trudovoj dogovor.* — 656 s.
8. Lyutov N. L. *Vsemirnaya trgovaya organizaciya: perspektivy uchastiya v ustanovlenii mezhdunarodnyh trudovyh standartov // Trudovoe pravo.* — 2009. — № 7. — S. 80—84.
9. Lyutov N. L. *Mezhdunarodnye trudovye standarty i mezhdunarodnaya trgovlya v usloviyah globalizacii: problemy vzaimodejstviya (v svete vstupleniya Rossii v VTO) // Rossijskij yuridicheskij zhurnal.* — 2013. — № 6 (93). — S. 127—134.
10. *Mezhdunarodnaya konferenciya truda, 104-ya sessiya, 2015 g. Doklad General'nogo direktora MBT «Iniciativa stoletiya, kasayushchayasya budushchego sfery truda».* — Zheneva : MBT, 2015.
11. *Neustojchivaya zanyatost' v Rossijskoj Federacii: teoriya i metodologiya vyyavleniya, ocenivanie i vektor sokrashcheniya / pod red. V. N. Bobkova.* — M. : Knorus, 2018. — 342 s.
12. Nurtidinova A. F., Chikanova L. A. *Differenciaciya regulirovaniya trudovyh otnoshenij kak zakonomernost' razvitiya trudovogo prava // Zhurnal rossijskogo prava.* — 2015. — № 6. — S. 68—82.
13. Orlovskij Yu. P. *Edinstvo i differenciaciya trudovogo zakonodatel'stva // Pravo cheloveka na zhizn' i garantii ego realizacii v sfere truda i social'nogo obespecheniya : materialy nauchno-prakticheskoy konferencii / pod red. K. N. Gusova.* — M., 2008. — S. 27—30.
14. *Problemy differenciacii v pravovom regulirovanii otnoshenij v sfere truda i social'nogo obespecheniya : materialy nauchno-prakticheskoy konferencii / pod red. K. N. Gusova.* — M., 2009. — 544 s.
15. *Rabotat' radi luchshego budushchego / Global'naya komissiya po voprosam budushchego sfery truda : Mezhdunarodnoe byuro truda.* — Zheneva : MBT, 2019. — URL: https://www.ilo.org/wcmsp5/groups/public/-/dgreports/-/cabinet/documents/publication/wcms_662472.pdf.
16. Tarusina N. N., Lushnikov A. M., Lushnikova M. V. *Social'nye dogovory v prave : monografiya.* — M. : Prospekt, 2017. — 480 s.
17. Tomashevskij K. L. *Opredelenie trudovogo otnosheniya: ot doktrinal'nyh razrabotok k legal'nomu zakrepleniyu v gosudarstvah — chlenah EAES // Trudovoe pravo v Rossii i za rubezhom.* — 2018. — № 1. — S. 3—6.
18. Chesalina O. V. *Rabota na osnove internet-platfom (crowdwork i work on demand via apps) kak vyzov trudovomu i social'nomu pravu // Trudovoe pravo v Rossii i za rubezhom.* — 2017. — № 1. — S. 52—55.

Цифровизация: уголовно-правовые риски в сфере экономики¹

Аннотация. Любая промышленная революция не только открывает новые возможности для общества и государства, но и наделяет преступников не существовавшими ранее способами и инструментами для совершения преступлений. Четвертая промышленная революция характеризуется автоматизацией и роботизацией производства, искусственным интеллектом, 3D-печатью, созданием новых материалов и технологий (биотехнологий и информационных технологий) и т.д.

Одним из объектов уголовно-правовой охраны, угроза причинения вреда которому создается в результате цифровизации, выступает экономика (общественные отношения, возникающие в связи с обеспечением нормального функционирования экономики как единого народно-хозяйственного комплекса). В настоящее время можно выделить такие киберугрозы для экономики, как атаки на банки, на брокера, на расчетную систему, хищения через интернет-банкинг и некоторые другие действия, совершаемые посредством использования вредоносных программ. Их основной целью выступает неправомерное завладение чужим имуществом. Наиболее распространенными способами совершения хищения являются ручной перевод средств с компьютера владельца счета через удаленный доступ, автозалив, метод социального инжиниринга, применение программы-вымогателя, неправомерное использование бренда и др.

В условиях цифровизации перед наукой уголовного права стоит задача разработки модели системного обновления отечественного уголовного законодательства, выработки общих правил и четких критериев его осуществления, а не спонтанного ответа на сиюминутные потребности правоприменителя путем конструирования специальных составов киберпреступлений.

Ключевые слова: цифровизация, киберпреступления, уголовно-правовые риски, криптовалюта, блокчейн, четвертая промышленная революция, информационные технологии; программы-вымогатели, атаки на банки.

DOI: 10.17803/1994-1471.2019.103.6.108-116

¹ Работа выполнена при финансовой поддержке РФФИ по договору № 18-29-16158/18.

© Арямов А. А., Грачева Ю. В., 2019

* *Арямов Андрей Анатольевич*, доктор юридических наук, профессор, профессор кафедры уголовного права Российского государственного университета правосудия
aaryamov65@yandex.ru

117418, Россия, г. Москва, ул. Новочеремушкинская, д. 69

** *Грачева Юлия Викторовна*, доктор юридических наук, профессор, профессор кафедры уголовного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)

uvgracheva@mail.ru

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

ВМЕСТО ВВЕДЕНИЯ

Четвертая промышленная революция обусловила появление:

- 1) автоматизации и роботизации производства, армии и всех сторон общественной жизни. При этом под робототехникой понимаются программируемые машины, которые могут автономно или автоматически выполнять те или иные действия; надо иметь в виду, что робототехника не является синонимом искусственного интеллекта. Последний предназначен для выполнения задач, которые могут быть решены без участия интеллекта человека;
- 2) 3D-печати. В ее основе лежит технология Additive Manufacturing, т.е. аддитивное² изготовление;
- 3) «производства новых материалов, включая материалы с заранее спроектированными свойствами, композитные материалы и т.п. Необходимость появления широчайшей гаммы новых материалов обусловлено, с одной стороны, требованиями широкого внедрения экономичной, эффективной 3D-печати, а с другой — развитием микроэлектроники, биотехнологий и т. п.»³;
- 4) биотехнологий, в том числе:
 - индустрии индивидуализированных лекарств;
 - регенеративной медицины, использующей возможности 3D-печати для производства донорских органов;
 - биоинформатики;
- 5) информационных технологий, включающих:

- большие данные (big data). Большие данные — «это сбор, хранение, оцифровка, обработка и предоставление в удобном для пользователя виде в любое время и в любой точке всей совокупности сведений о тех или иных событиях, процессах, явлениях и т.п. Ключевым в больших данных является то, что они позволяют работать именно со всей информацией в режиме онлайн. Определяющим здесь выступает слово «всей». Сами по себе большие данные являются важнейшим государственным и корпоративным активом, который при должном использовании обеспечивает их владельцам интеллектуальное превосходство и деловое доминирование»⁴;
- когнитивные вычисления и экспертные системы. Как отмечается в науке, «в основу когнитивных вычислений заложены программы, моделирующие и имитирующие некоторые известные психофизиологические процессы человека. За счет этого созданы программы, обладающие возможностями совершенствования, и умеющие учитывать при решении тех или иных задач ошибки»⁵;
- «облачные» и распределенные вычисления, т.е. информационно-технологическая модель обеспечения повсеместного и удобного доступа с использованием сети Интернет к общему набору конфигурируемых вычислительных ресурсов («облаку»), устройствам хранения данных, приложениям и сервисам, которые могут быть оперативно предоставлены и освобождены от нагрузки с минимальными эксплуатационными затратами или практически без участия провайдера»⁶;

² Аддитивное производство — группа технологических методов производства изделий и прототипов, основанная на поэтапном добавлении материала на основу в виде плоской платформы или осевой заготовки (см.: URL: https://ru.wikipedia.org/wiki/%D0%90%D0%B4%D0%B4%D0%B8%D1%82%D0%B8%D0%B2%D0%BD%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D0%B8%D0%B7%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%BE (дата обращения: 15.03.2019).

³ Ларина Е., Овчинский В. Русское чудо XXI века // URL: <http://zavtra.ru/blogs/russkoe-chudo-xxi-veka> (дата обращения: 15.03.2019).

⁴ Ларина Е., Овчинский В. Указ. соч.

⁵ Ларина Е., Овчинский В. Указ. соч.

⁶ Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы» // СЗ РФ. 2017. № 20. Ст. 2901.

— блокчейн — компьютерная технология, построенная на особой системе шифрования, по существу — информационная база данных, в которой записи группируются в блоки, где каждый блок связан со следующим с помощью использования криптографической подписи. Блокчейн позволяет эффективно сохранять данные, но сам по себе не обеспечивает их достоверность, поскольку они самостоятельно вводятся пользователями. Последние создают записи, а особые субъекты, майнеры⁷, проверяют их и группируют в блоки, после чего посредством своих мощностей пытаются рассчитать ключ к данному блоку. Справившийся с этой задачей майнер включает полученную информацию в блок, тем самым гарантирует ее достоверность. Выделяют: открытый публичный блокчейн⁸; консорциумный (комбинированный) блокчейн; закрытый частный блокчейн. Основные чертами технологии блокчейн являются: децентрализованность, анонимность, автономность, использование криптографии, присвоение каждой транзакции особых меток времени. Блокчейн-приложения разделяются на три категории в зависимости от уровня разработки: 1.0 — криптовалюта; 2.0 — модели умных контрактов; 3.0 — практически автономные смарт-контракты⁹.

КИБЕРУГРОЗЫ И УГОЛОВНО-ПРАВОВЫЕ ПРОБЛЕМЫ

Чем выше технологический уровень государства и общества, чем глубже информационно-коммуникационные технологии проникли во все сферы жизни общества, тем более уязвимыми

они становятся для организованной преступности и террористов¹⁰. Каждая высокая технология имеет тройное применение: гражданское, военное и криминальное. В связи с этим любая промышленная революция не только открывает новые возможности для общества и государства, но и наделяет преступников не существовавшими ранее способами и инструментами для совершения преступлений, порождает новые угрозы объектам уголовно-правовой охраны.

Киберугрозы затрагивают все общество в целом, и их невозможно ликвидировать полностью в связи с тем, что цифровые технологии успешно работают в силу своей открытости, а это сопряжено с риском. Однако уголовному праву под силу выявить эти угрозы и разработать уголовно-правовой механизм по их минимизации.

Одним из объектов уголовно-правовой охраны, которому может быть создана угроза причинения вреда в результате цифровизации, выступает экономика (общественные отношения, характеризующие нормальное функционирование экономики как единого народно-хозяйственного комплекса). В настоящее время выявлены следующие виды киберугроз:

1) *атаки на банки*. Главной мишенью киберпреступников в этой сфере были небольшие региональные банки. Целенаправленные атаки на них, как правило, происходят с использованием методов социального инжиниринга.

Начиная с 2013 г. несколько разных групп русскоговорящих хакеров атакуют банки и платежные системы. Делают это они очень успешно. Общая сумма хищений, к которым причастны эти мошенники, составляет более 1 млрд

⁷ Лицо, подтверждающее транзакцию, получающее вознаграждение и комиссию.

⁸ Публичный блокчейн не требует идентификации: любое лицо может вписать данные без разрешения и любое лицо может прочитать эти данные. Кроме того, эта платформа не имеет фиксированного перечня майнеров, им может быть любое лицо. Частный блокчейн предъявляет требования как к идентификации, так и к майнерам.

⁹ См.: Новгородская В. Б. Новые технологии (блокчейн / искусственный интеллект) на службе права : научно-методическое пособие / под ред. Л. А. Новоселовой. М., 2019. С. 7, 9, 11, 13, 14, 18.

¹⁰ См.: Национальная стратегия кибербезопасности 2016—2021 гг. (Великобритания) // URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643426/Russian_translation_-_National_Cyber_Security_Strategy_2016.pdf (дата обращения: 17.03.2019).

руб. (по состоянию на вторую половину 2014 г.). В конце 2015 г. и начале 2016 г. группа Vuhtrap похитила у 13 банков 1,8 млрд руб. Средняя сумма хищения составила 143 млн руб.¹¹;

2) *атаки на брокера*. В 2015 г. была проведена первая успешная атака на брокера, которая вызвала большой резонанс среди участников финансового рынка. Для этой атаки «использовался троян Corkow (также известный как Metel). Он предоставляет удаленный доступ к системе, что позволяет злоумышленнику запускать программы, управлять клавиатурой и мышкой параллельно с оператором системы. В результате несанкционированного доступа к терминалу торговой системы было выставлено пять заявок на покупку 437 млн долл.»¹² и две заявки на продажу 97 млн долл. Однако была исполнена только часть заявок, в результате было куплено 158,536 тыс. и продано 93,925 тыс. долл. США. Указанные действия вызвали очень большую волатильность в течение 6 мин, что привело к причинению ущерба банку в размере 300 млн руб. Через 14 мин после первой заявки хакер дал команду Corkow на удаление своих следов и вывод системы из строя¹³;

3) *атаки на расчетную систему*. Так, 16 августа 2015 г. произошел инцидент, в результате которого через банкоматы было похищено около 500 млн руб. Он затронул около 15 крупных банков — участников одной из российских расчетных систем, которая объединяет около 250 банков¹⁴. Были использованы вредоносные программы, хорошо известные антивирусным компаниям, которые очень сложно вовремя обнаружить стандартными средствами антивирусной защиты. Эти вредоносные программы предоставляли удаленный доступ к нужным системам внутризащищенных сетей и давали атакующим все возможности, доступные сотрудникам финансовых учреждений;

4) *хищения через интернет-банкинг*. Практически все стандартные меры безопасности, применяемые банками, — защищенные токены (ключи для авторизации пользователя), отслеживание смены оборудования и мест отправки платежных поручений, СМС-подтверждение и т.п. — можно обойти. Наиболее распространенными способами подобных хищений выступают:

- ручной перевод посредством удаленного доступа с компьютера владельца счета денежных средств. Для того чтобы обойти защиту электронных цифровых подписей (ЭЦП), хранимых на защищенных токенах, а также систему обнаружения смены компьютера владельца счета, используется удаленное подключение к компьютеру владельца счета, с которого совершается мошеннический перевод средств. Процесс формирования платежного поручения начинается после того, как владелец счета подключил к ЭВМ токен с ЭЦП. При удаленном подключении преступника работа владельца компьютера не нарушается и может проходить одновременно. Удаленный доступ будет предоставлен атакующему, даже если все входящие соединения к компьютеру владельца счета будут запрещены. Это обеспечивается за счет того, что средства удаленного доступа сами устанавливают исходящее соединение с сервером преступника, а злоумышленник, используя исходящее соединение, подключается к компьютеру владельца счета. Исходящие соединения с компьютером владельца счета, как правило, разрешены для обеспечения нормальной работы в сети «Интернет»;
- автоматический перевод (автозалив). Данный вариант совершения платежа является наиболее совершенным. Автозалив можно сделать двумя способами. Первый — непосредственно перед подписанием платежного поручения владельцем счета вредоносная

¹¹ См.: Овчинский В. С. Криминология цифрового мира. М. : Норма: Инфра-М, 2018. С. 114—115.

¹² Черных Е. Киберпреступность и наши телефоны // URL: <http://crimescience.ru/?p=9980> (дата обращения: 17.03.2019).

¹³ См.: Черных Е. Указ. соч.

¹⁴ См.: Овчинский В. С. Указ. соч. С. 115.

- программа заменит реквизиты платежа, при этом на экране будут отображаться данные, внесенные владельцем счета. В результате владелец счета подпишет уже измененное платежное поручение и отправит его в банк. Второй способ — вредоносная программа дожидается подключения токена с ЭЦП, сама запустит систему интернет-банкинга, войдет с использованием логина (пароля) владельца счета, сформирует платежное поручение и отправит его в банк. Для того чтобы троянская программа в автоматическом режиме перевела денежные средства, преступник должен подготовить специальный файл настроек с указанием реквизитов для перевода. Данный файл настроек будет скачан вредоносной программой по команде с сервера управления ботнета¹⁵;
- метод социального инжиниринга предполагает использование троянской программы для перенаправления пользовательских запросов к банковским сайтам на мошеннический сайт со страницами, внешне копирующими настоящий сайт банка. Фишинговый сайт используется для получения конфиденциальных данных пользователей: логина (пароля), номера телефона владельца счета. Переводы денежных средств необходимо подтверждать одноразовым кодом, который может быть получен владельцем счета по СМС, со скрэтч-карты или иным способом. Для получения кода подтверждения мошенник показывает фишинговые страницы, требующие ввести код подтверждения
- под разными предложениями, например для отмены мошеннической операции. При нажатии на любую из кнопок (аннулировать или подтвердить) код подтверждения будет отправлен преступнику, и он сможет завершить перевод денежных средств. Если пользователь не вводит полученный код подтверждения, то преступник, используя номер телефона, который будет указан пользователем на фишинговом сайте, осуществит звонок владельцу счета от имени банка. Цель звонка — уговорить пользователя ввести код подтверждения перевода денежных средств на фишинговом сайте либо продиктовать код по телефону;
- программы-вымогатели. В России эта угроза стала серьезной проблемой для бизнеса относительно недавно. Основной задачей таких программ является шифрование файлов надежным методом, чтобы расшифровать их можно было только при наличии специального секретного ключа, находящегося у вымогателя. Главное — это «зашифровать не просто файлы, а базы данных, рабочие документы, резервные копии и т.д.»¹⁶ После того как файлы зашифрованы, приходит уведомление, в котором сообщается, сколько и куда необходимо перевести денег, чтобы получить ключ расшифровки. Как правило, оплата производится в биткоинах. Больше всего компании страдают, когда злоумышленники шифруют базы 1С:Бухгалтерии, общие файловые серверы, данные резервных копий. Как отмечает И. Сачков, «основной

¹⁵ Ботнет (от слов *robot* и *network*) — компьютерная сеть, состоящая из некоторого количества хостов с запущенными ботами — автономным программным обеспечением. Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на устройство жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов зараженного компьютера. Обычно используются для нелегальной или неодобряемой деятельности — рассылки спама, перебора паролей на удаленной системе, атак на отказ в обслуживании (DoS- и DDoS-атаки). Боты как таковые не являются вирусами. Они представляют собой набор программного обеспечения, который может состоять из вирусов, брандмауэров, программ для удаленного управления компьютером, а также инструментов для скрытия от операционной системы (см.: URL: <https://ru.wikipedia.org/wiki/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82> (дата обращения: 17.03.2019)).

¹⁶ Сачков И. Зашифрованный мир: как работает WannaCry и что умеют программы-вымогатели? // URL: <https://www.forbes.ru/tehnologii/344285-zashifrovannyi-mir-kak-rabotaet-wannacry-i-cto-umeyut-programmy-vymogateli> (дата обращения: 17.03.2019).

способ распространения таких программ — рассылки по электронной почте вложений под видом банковских выписок, счетов, уведомлений о вызове в суд и т.п.»¹⁷;

— неправомерное использование бренда. Наиболее яркий пример — использование бренда для проведения фишинговых атак на клиентов, партнеров или даже внутренних сотрудников компании. Сейчас многие компании — банки, онлайн-магазины, такси, рестораны и т.д. — выходят на рынок со своими мобильными приложениями. Мошенники используют этот тренд, создавая фейковые мобильные приложения, которые пользователи устанавливают, среагировав на хорошо узнаваемые бренды и символику. Как правило, все они становятся жертвами мошеннических или вредоносных программ. Это не только наносит вред пользователям, скачавшим подобные приложения, но и подрывает доверие к компаниям, которые не уделяют должного внимания защите своих брендов.

В связи с развитием информационных технологий на мировом финансовом рынке появились виртуальные финансовые активы, созданные на основе технологии блокчейн, — криптовалюты, т.е. цифровые записи со своим криптографическим кодом в определенной информационной системе, существующей только в виртуальном пространстве. Криптовалюта имеет децентрализованный характер, не эмитирована государством, обладает рядом

преимуществ по сравнению с фиатными деньгами: анонимность, минимальный процент по транзакциям, неподконтрольность публичной власти и т.д. Эти преимущества обуславливают уголовно-правовые риски использования криптовалюты для анонимного финансирования терроризма, незаконного оборота наркотических средств (психотропных веществ), оружия, порнографических материалов, легализации имущества¹⁸.

В судебной практике не вызывает сложностей квалификация преступлений, в которых криптовалюта является средством их совершения, сложности появляются тогда, когда она выступает предметом преступления. Это обусловлено тем, что в российском законодательстве до сих пор не определена юридическая природа криптовалюты, поэтому в теории уголовного права предлагаются разные варианты уголовно-правовой оценки подобных деяний, ни один из которых не основан на буквальном толковании уголовного закона¹⁹.

Федеральный закон «О цифровых финансовых активах», который в том числе должен был определить правовой статус криптовалюты, пока не принят (идет обсуждение проекта, однако примечательно, что Центробанк предложил исключить из него всякое упоминание о криптовалютах). Между тем депутаты Государственной Думы РФ только планируют в течение 2019 г. принять отдельный закон о криптовалютах²⁰. В ГК РФ уже внесены изменения — ст. 128 ГК РФ дополнена цифровыми правами²¹, а в ст. 141.1²²

¹⁷ Сачков И. Указ. соч.

¹⁸ См.: Уфимцева В. А. Уголовно-правовые риски использования криптовалюты // Уголовное право: стратегия развития в XXI веке : материалы XVI Междунар. науч.-практ. конференции. М., 2019. С. 140—141.

¹⁹ См.: Уфимцева В. А. Указ. соч. С. 145—146.

²⁰ URL: https://fomag.ru/news-streem/gosduma_rf_otlozhila_vtoroe_chtenie_zakonoproekta_o_tsifrovyykh_aktivakh/ (дата обращения: 24.03.2019).

²¹ Некоторые ученые негативно оценивают отнесение цифровых прав к имущественным правам в связи с тем, что, по их мнению, «сложно понять, как цифровой код может быть отнесен к категории имущественного права, не являясь по своей сути правовым требованием, которое могло бы обращаться в гражданском обороте как разновидность прав» (Правовое регулирование экономических отношений в современных условиях развития цифровой экономики. М. : Юстицинформ, 2019. 376 с.).

²² Цифровыми правами признаются названные в таком качестве в законе обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам. Осуществление, распоряжение, в том

эти цифровые права разъясняются. Изменения вступят в силу с 1 октября 2019 г.²³ С этого момента неправомерные действия в отношении цифровых прав будут охватываться теми составами преступлений, в которых имущество закреплено в качестве предмета.

ВМЕСТО ЗАКЛЮЧЕНИЯ

Приведен далеко не полный перечень киберугроз в финансовой сфере, основной целью которых является неправомерное завладение чужим имуществом или конфиденциальной информацией посредством использования вредоносных программ. В этой связи некоторые ученые полагают, что, с одной стороны, подобный способ не получил должного отражения в УК РФ, несмотря на наличие, например, п. «г» ч. 3 ст. 158, 159.3, ст. 159.6. С другой стороны, нет единства

в оценке неправомерного доступа к чужой информационной системе кредитных учреждений (частных лиц) с намерением завладения чужим имуществом²⁴, в частности образуется ли совокупность преступлений, предусмотренных ст. 159.6 и ст. 272 УК РФ?²⁵ Кроме того, в теории уголовного права предлагается дополнить УК РФ самостоятельной «формой хищения с новым способом его совершения — использованием компьютерных технологий»²⁶. Не ставя целью проанализировать это предложение, отметим следующее. В условиях цифровизации перед доктриной уголовного права стоит задача скорейшей разработки модели системного обновления отечественного уголовного законодательства, выработки общих правил и четких критериев его осуществления, а не спонтанного ответа на актуальные потребности правоприменителя путем конструирования специальных составов киберпреступлений²⁷.

БИБЛИОГРАФИЯ

1. *Иногамова-Хегай Л. В.* Квалификация преступлений с использованием компьютерных технологий // Уголовное право: стратегия развития в XXI веке : материалы XVI Международной научно-практической конференции. — М., 2019.
2. *Ларина Е., Овчинский В.* Русское чудо XXI века // URL: <http://zavtra.ru/blogs/russkoe-chudo-xxi-veka>.
3. *Новгородская В. Б.* Новые технологии (блокчейн / искусственный интеллект) на службе права: научно-методическое пособие / под ред. Л. А. Новоселовой. — М., 2019.
4. *Овчинский В. С.* Криминология цифрового мира : учебник для магистратуры. — М. : Норма: Инфра-М, 2018.

числе передача, залог, обременение цифрового права другими способами или ограничение распоряжения цифровым правом возможны только в информационной системе без обращения к третьему лицу (ч. 1 ст. 141.1 ГК РФ).

²³ Федеральный закон от 18.03.2019 № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» // СЗ РФ. 2019. № 12. Ст. 1224.

²⁴ См.: *Иногамова-Хегай Л. В.* Квалификация преступлений с использованием компьютерных технологий // Уголовное право: стратегия развития в XXI веке. С. 52—55.

²⁵ Пленум Верховного Суда РФ считает, что мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по ст. 272, 273 или 274.1 УК РФ (п. 20 постановления Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»).

²⁶ *Иногамова-Хегай Л. В.* Указ. соч. С. 54—55.

²⁷ См.: *Русскиевич Е. А.* О концепции «минималистической цифровизации» Особенной части УК РФ // Уголовное право: стратегия развития в XXI веке. С. 110—116.

5. Правовое регулирование экономических отношений в современных условиях развития цифровой экономики : монография / отв. ред. В. А. Вайпан, М. А. Егорова. — М. : Юстицинформ, 2019.
6. Русскиевич Е. А. О концепции «минималистической цифровизации» особенной части УК РФ // Уголовное право: стратегия развития в XXI веке : материалы XVI Международной научно-практической конференции. — М., 2019.
7. Сачков И. Зашифрованный мир: как работает WannaCry и что умеют программы-вымогатели? // URL: <https://www.forbes.ru/tehnologii/344285-zashifrovannyj-mir-kak-rabotaet-wannacry-i-cto-umejut-programmy-vymogateli>.
8. Уфимцева В. А. Уголовно-правовые риски использования криптовалюты // Уголовное право: стратегия развития в XXI веке : материалы XVI Международной научно-практической конференции. — М., 2019.
9. Черных Е. Киберпреступность и наши телефоны // URL: <http://crimescience.ru/?p=9980>.

Материал поступил в редакцию 6 мая 2019 г.

DIGITALIZATION: CRIMINAL LAW RISKS IN THE ECONOMY²⁸

ARYAMOV Andrey Anatolievich, Doctor of Law, Professor, Professor of the Department of Criminal Law of the Russian State University of Justice
aaryamov65@yandex.ru
117418, Russia, Moscow, ul. Novocheriomushkinskaya, d. 69

GRACHEVA Yulia Viktorovna, Doctor of Law, Professor, Professor of the Department of Criminal Law of the Kutafin Moscow State Law University (MSAL)
uvgracheva@mail.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

Abstract. *Any industrial revolution not only opens up new opportunities for society and the state, but also endows criminals with previously non-existing methods and tools for committing crimes. Automation and production robotization, artificial intelligence, 3D printing, the creation of new materials and technologies (biotechnologies and information technologies), etc characterize the fourth industrial revolution.*

One of the objects of the criminal law protection under threat of harm due to digitalization is the economy (public relations arising from ensuring the normal functioning of the economy as a single national economic complex). At present, it is possible to distinguish such cyber threats for the economy as attacks on banks, on a broker, on a settlement system, embezzlement through Internet banking and some other actions carried out through the use of malicious programs. Their main purpose is misappropriation of other people's property. The most common methods of embezzlement are the manual transfer of funds from the computer of the account owner through the remote access, automatic software upload, social engineering method, the use of an ransomware program, illegal use of the brand, etc.

In the conditions of digitalization, the science of criminal law faces the task of developing a model for systematic updating of domestic criminal legislation, developing general rules and clear criteria for its implementation, rather than a spontaneous response to the immediate needs of a law enforcer by designing special cybercrime compounds.

Keywords: *digitalization, cybercrime, criminal law risks, cryptocurrency, blockchain, fourth industrial revolution, information technology; extortion programs, attacks on banks.*

²⁸ The work is carried out with the financial support of the Russian Foundation for Basic Research, Contract No. 18-29-16158 / 18.

REFERENCES (TRANSLITERATION)

1. Inogamova-Hegaj L. V. Kvalifikaciya prestuplenij s ispol'zovaniem komp'yuternyh tekhnologij // Uголовное право: strategiya razvitiya v XXI veke : materialy XVI Mezhdunarodnoj nauchno-prakticheskoj konferencii. — M., 2019.
2. Larina E., Ovchinskij V. Russkoe chudo XXI veka // URL: <http://zavtra.ru/blogs/russkoe-chudo-xxi-veka>.
3. Novgorodskaya V. B. Novye tekhnologii (blokchejn / iskusstvennyj intellekt) na sluzhbe prava: nauchno-metodicheskoe posobie / pod red. L. A. Novoselovoj. — M., 2019.
4. Ovchinskij V. S. Kriminologiya cifrovogo mira : uchebnik dlya magistratury. — M. : Norma: Infra-M, 2018.
5. Pravovoe regulirovanie ekonomicheskikh otnoshenij v sovremennykh usloviyah razvitiya cifrovoj ekonomiki : monografiya / otv. red. V. A. Vajpan, M. A. Egorova. — M. : Yusticinform, 2019.
6. Russkevich E. A. O koncepcii «minimalisticheskoy cifrovizacii» osobennoj chasti UK RF // Uголовное право: strategiya razvitiya v XXI veke : materialy XVI Mezhdunarodnoj nauchno-prakticheskoj konferencii. — M., 2019.
7. Sachkov I. Zashifrovannyj mir: kak rabotaet WannaCry i chto umeyut programmy-vymogateli? // URL: <https://www.forbes.ru/tehnologii/344285-zashifrovannyj-mir-kak-rabotaet-wannacry-i-chto-umeyut-programmy-vymogateli>.
8. Ufimceva V. A. Uголовно-pravovye riski ispol'zovaniya kriptovalyuty // Uголовное право: strategiya razvitiya v XXI veke : materialy XVI Mezhdunarodnoj nauchno-prakticheskoj konferencii. — M., 2019.
9. Chernyh E. Kiberprestupnost' i nashi telefony // URL: <http://crimescience.ru/?p=9980>.

А. И. Чучаев*,
С. В. Маликов**

Ответственность за причинение ущерба высокоавтоматизированным транспортным средством: состояние и перспективы¹

Аннотация. В статье дается характеристика существующего в России нормативного правового регулирования ответственности за причинение вреда высокоавтоматизированным (беспилотным) транспортным средством (БТС). К наиболее значимым документам в настоящее время относятся: Конвенция о дорожном движении; Стратегия безопасности дорожного движения в Российской Федерации; «Дорожная карта» по совершенствованию законодательства и устранению административных барьеров в целях обеспечения реализации Национальной технологической инициативы по направлению «Автонет». Основное внимание уделено постановлению Правительства РФ, в котором указаны первые подходы к регулированию эксплуатации высокоавтоматизированных транспортных средств, названы субъекты, несущие ответственность в случае причинения вреда беспилотником. В общих чертах показаны принципы функционирования БТС и степень их автономности. Анализируются имеющиеся в отечественном уголовном праве подходы к ответственности лиц, управляющих БТС, и подходы, разрабатываемые в зарубежных странах применительно к регламентации эксплуатации высокоавтоматизированных транспортных средств. Указаны основные подходы к определению уголовно-правового запрета и выделены наиболее важные алгоритмы криминализации рассматриваемого деяния. Предлагается структура федерального закона о регулировании использования транспортных средств, оборудованных системой автоматического управления, на территории Российской Федерации.

Ключевые слова: беспилотные транспортные средства (БТС), транспортные преступления, правовое регулирование, преступление, правовая природа, криминализация, уголовная ответственность, субъект преступления, причинение вреда, проект закона.

DOI: 10.17803/1994-1471.2019.103.6.117-124

¹ Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16162.

© Чучаев А. И., Маликов С. В., 2019

* Чучаев Александр Иванович, доктор юридических наук, профессор, профессор кафедры уголовного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
toksha1@rambler.ru

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

** Маликов Сергей Владимирович, кандидат юридических наук, старший преподаватель кафедры уголовного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
s.v.malikov@yandex.ru

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

Цифровая революция в современном мире сопровождается не только компьютеризацией многих процессов, но и их автоматизацией. На транспорте частичная автоматизация вождения уже является стандартом в новых автомобилях. При этом под автоматизацией частного транспорта, эксплуатируемого в условиях дорог общего пользования, понимаются технологические средства управления, которые облегчают нагрузку на водителей, помогают им или даже заменяют их частично или полностью.

Внимание к развитию роботизированного автотранспорта вполне объяснимо. За счет его эксплуатации в народном хозяйстве достигается решение ряда задач, в том числе: осуществление перевозок грузов в опасных зонах (например, ставших очагами разного рода заражений), во время природных и техногенных катастроф или военных действий; снижение себестоимости пассажиро- и грузоперевозок за счет исключения из процесса транспортировки труда водителей; обеспечение ценовой доступности автотранспортных услуг для всех слоев населения в соответствии с транспортными стандартами; повышение эффективности использования транспортных магистралей и горюче-смазочных материалов в связи с централизованным управлением автомобильным потоком, возможностью сужения ширины дорожных полос; улучшение комфортности труда водителей-операторов; самостоятельное перемещение на автомобиле лиц, которые в настоящее время не допускаются к управлению транспортными средствами в силу ряда причин (например, ослабленное зрение, несовершеннолетний возраст и др.); существенное снижение аварийности, рисков и угроз безопасности на автомобильном транспорте, минимизация тяжких последствий в связи с исключением из этиологии дорожно-транспортных происшествий человеческого фактора

(по некоторым данным, аварийность на дорогах может снизиться на 70—80 %); значительное уменьшение вредного воздействия транспорта на окружающую среду и др.²

Появление на дорогах общего пользования беспилотных транспортных средств ставит ряд вопросов, связанных с их безопасностью, в частности с определением субъектов ответственности за возможные дорожно-транспортные происшествия с участием таких автомобилей. Большинство стран, занимающихся разработкой беспилотных транспортных средств, идут по пути законодательного закрепления необходимости нахождения в салоне беспилотного автомобиля человека, который в случае экстренной ситуации сможет взять управление транспортным средством на себя. Такой подход основывается на положениях Венской конвенции о дорожном движении 1968 г., установившей, что каждое транспортное средство или состав транспортных средств, которые находятся в движении, должны иметь водителя (ст. 8)³.

Наряду с этим зарубежное законодательство, как правило, не регламентирует порядок получения прав на управление беспилотными автомобилями, не содержит норм, предусматривающих ответственность за дорожно-транспортные преступления с их участием. В настоящее время только запускается процесс формирования требований к внедрению автономных автомобилей на дорогах общего пользования, основными из которых является обязательное наличие водителя в салоне, возможность переключения беспилотников на ручное управление⁴.

В Стратегии безопасности дорожного движения в Российской Федерации на 2018—2024 годы, утвержденной распоряжением Правительства РФ от 8 января 2018 г. № 1-р⁵, отмечается приоритетность использования современных технологий в деятельности по обе-

² Подробно об этом см.: Коробеев А. И., Чучаев А. И. Беспилотные транспортные средства: новые вызовы общественной безопасности // Lex Russica. 2019. № 2. С. 9—29.

³ Конвенция о дорожном движении (вместе с Техническими условиями, касающимися автомобилей и прицепов) (заключена в г. Вене 8 ноября 1968 г.) // СПС «КонсультантПлюс».

⁴ См.: Штаге Д. Автоматизированное вождение и спорные ситуации // Уголовное право: стратегия развития в XXI веке. С. 3—7.

⁵ СЗ РФ. 2018. № 5. Ст. 774.

спечению безопасности дорожного движения (интеллектуальных транспортных систем, систем автоматизации процесса управления), что направлено на снижение аварийности на дорогах, увеличение безопасности водителей и пассажиров в автомобилях с полуавтоматическим (или автоматическим) управлением.

Распоряжением Правительства РФ от 29 марта 2018 г. № 535-р «Об утверждении плана мероприятий («дорожной карты») по совершенствованию законодательства и устранению административных барьеров в целях обеспечения реализации Национальной технологической инициативы по направлению «Автонет»» предусмотрены мероприятия по установлению особенностей обучения водителей эксплуатации автомобилей с высокой степенью автоматизации управления⁶. В документе особо отмечается, что ограничения в рамках реализации плана мероприятий «Автонет» обусловлены отсутствием юридического и технического регулирования, которое необходимо для правового обеспечения вывода на рынок новых продуктов и субъектов новых видов предпринимательской деятельности, для реализации новых бизнес-моделей, а также отсутствием норм, которые обеспечивают условия для разработки и продвижения передовых технологических решений, существованием и применением нормативных правовых актов и документов по стандартизации, положения которых не отвечают современным научно-технологическим вызовам и приоритетам научно-технологического развития, сдерживают вывод на рынок новых продуктов и услуг.

Первой попыткой регламентации отношений в сфере использования беспилотных транспортных средств, в том числе затрагивающей вопросы ответственности, является постановление Правительства РФ от 26 ноября 2018 г. № 1415 «О проведении эксперимента по опытной эксплуатации на автомобильных дорогах общего пользования высокоавтоматизированных транспортных средств»⁷. В нем определяются субъекты возникающих правоотношений с рас-

пределением ответственности в случае причинения вреда жизни и здоровью людей, а также имущественного ущерба. К таковым отнесены:

- а) собственник высокоавтоматизированного транспортного средства — юридическое лицо, которому на праве собственности принадлежит высокоавтоматизированное транспортное средство и которое участвует в проведении эксперимента на добровольной основе;
- б) водитель высокоавтоматизированного транспортного средства — физическое лицо, находящееся во время проведения эксперимента на месте водителя высокоавтоматизированного транспортного средства, активирующее автоматизированную систему вождения высокоавтоматизированного транспортного средства и контролирующее движение этого транспортного средства в автоматизированном режиме управления, а также осуществляющее управление высокоавтоматизированным транспортным средством в режиме ручного управления. Водитель высокоавтоматизированного транспортного средства является водителем в соответствии с положениями Правил дорожного движения Российской Федерации, утвержденных постановлением Правительства РФ от 23 октября 1993 г. № 1090.

Ответственность за дорожно-транспортные и иные происшествия на автомобильных дорогах России, произошедшие с участием высокоавтоматизированного транспортного средства при проведении эксперимента, при отсутствии виновных действий других участников дорожного движения, приведших к данному дорожно-транспортному или иному происшествию на автомобильной дороге, несет собственник высокоавтоматизированного транспортного средства (п. 18 постановления Правительства РФ № 1415).

Толкование этой нормы и иных положений анализируемого постановления позволяет констатировать, что водитель понимается как участник дорожного движения, чьи виновные дей-

⁶ СЗ РФ. 2018. № 16 (ч. 2). Ст. 2393.

⁷ СПС «КонсультантПлюс».

ствия могут также привести к дорожно-транспортным происшествиям, причиняющим вред имуществу, здоровью и жизни других лиц, поскольку он обязан активировать автоматизированную систему вождения высокоавтоматизированного транспортного средства, контролировать его движение в автоматизированном режиме управления, а также осуществлять управление высокоавтоматизированным транспортным средством в режиме ручного управления. В то же время такой подход оставляет вопрос о том, что понимать под виновными действиями водителя. Вероятно, имеются в виду неправомерные действия по переходу на ручное управление транспортным средством в случаях, когда не было необходимости предотвращать дорожно-транспортное происшествие, что привело к причинению вреда, а также непринятие ручного управления транспортным средством в случаях, когда была необходимость предотвратить дорожно-транспортное происшествие. Сложности порождаются отсутствием законодательного определения понятия «управление транспортным средством», что затрудняет оценку «вклада» водителя в процесс управления автотопитируемым транспортом, определение его вины, характера влияния на наступление дорожно-транспортных последствий.

Заложенный в постановлении Правительства РФ № 1415 подход свидетельствует о большей ответственности водителя, нежели собственника, поскольку на первого возложена обязанность контроля за соблюдением правил дорожного движения и предотвращения дорожно-транспортных происшествий. Собственник высокоавтоматизированного транспортного средства в рамках эксперимента несет ответственность скорее за сбои в программно-аппаратных средствах, которые не могут быть устранены водителем. В пользу данного утверждения свидетельствует также то, что привлечение к ответственности за дорожно-транспортные преступления автопроизводителей, организации, отвечающие за надлежащие состояние улично-дорожной сети, в рамках действующе-

го российского уголовного законодательства невозможно ввиду отсутствия в нем уголовной ответственности юридических лиц.

На это обстоятельство указывает, в частности, то, что до дня подачи заявки на получение в отношении высокоавтоматизированного транспортного средства заключения о соответствии транспортного средства с внесенными в его конструкцию изменениями требованиям безопасности заявитель (собственник) должен застраховать и поддерживать застрахованным в период проведения опытной эксплуатации риск ответственности по обязательствам, возникающим вследствие причинения вреда жизни, здоровью или имуществу других лиц в пользу третьих лиц на сумму 10 млн руб. в отношении каждого высокоавтоматизированного транспортного средства, т.е. речь идет лишь о гражданско-правовой ответственности.

Субъектом уголовной ответственности по ст. 264 УК РФ может выступать водитель, который при необходимости берет на себя управление.

Рассматриваемое постановление Правительства РФ представляет собой лишь первую попытку закрепления и распределения ответственности за ущерб, причиняемый беспилотными транспортными средствами. Можно констатировать, что нормативные документы, регулирующие эксплуатацию беспилотных автомобилей, находятся в стадии разработки.

Следует иметь в виду, что развитие беспилотных транспортных средств приведет их к полной автономности. В связи с этим в теории выделяются степени автономности автомобилей. По классификации SAE International (сообщество автомобильных инженеров) систем помощи водителю, или ADAS (Advanced Driver Assistance System)⁸, существует шесть классов автономности:

- уровень 0 — полностью ручное управление с возможностью предупреждения об опасных ситуациях на дороге (наличие системы уведомлений);
- уровень 1 — водитель должен быть готов в любой момент взять управление на себя;

⁸ См.: Стандарт SAE J3016 // URL: https://www.sae.org/binaries/content/assets/cm/content/news/press-releases/pathway-to-autonomy/automated_driving.pdf (дата обращения: 22.04.2019).

- могут присутствовать следующие автоматизированные системы: круиз-контроль (ACC, Adaptive Cruise Control), автоматическая парковочная система и система предупреждения о сходе с полосы (LKA, Lane Keeping Assistance);
- уровень 2 — водитель должен реагировать, если система не смогла справиться самостоятельно. Автоматика управляет ускорением, торможением и рулением; система может быть отключена;
 - уровень 3 — водитель может не контролировать машину на дорогах с «предсказуемым» движением (например, автобаны), но должен быть готов взять управление на себя;
 - уровень 4 — аналогичный 3-му уровню, но уже не требует внимания водителя;
 - уровень 5 — со стороны человека не требуется никаких действий, кроме старта системы и указания пункта назначения; автоматизированная система может обеспечить проезд до любой точки назначения, не запрещенной законом.

Визуально уровни могут быть представлены следующим образом (см. табл. 1):

Распределение ответственности между человеком и транспортным средством меняется в зависимости от выбранного уровня, указанного выше (см. рис. 1).

В 2016 г. Федеральным министерством транспорта и инфраструктуры Германии была создана комиссия по этике автоматизированного вождения. Ключевыми элементами ее доклада являются:

- автоматизированное и согласованное вождение выступает этическим императивом, если системы вызывают меньше аварий, чем водители-люди (положительный баланс риска);
- в опасных ситуациях защита человеческой жизни всегда должна иметь высший приоритет;
- в случае неизбежных аварийных ситуаций любое различие между людьми, основанное на личных особенностях (возраст, пол,

физическое или психическое состояние), недопустимо;

- в каждой ситуации при вождении должно быть четко регламентировано и ясно, кто отвечает за вождение: человек или компьютер;
- должны быть задокументированы и сохранены сведения, кто находился за рулем (для решения, среди прочего, возможных вопросов ответственности);
- водители должны всегда иметь возможность самостоятельно решать, следует ли передавать и использовать данные о транспортном средстве (суверенитет данных)⁹.

Чтобы понять дальнейшие потребности в области регулирования, необходимо выделить две точки зрения на нормативные требования. Во-первых, целесообразно внести поправки в правила дорожного движения для высокоавтоматизированных функций вождения. Во-вторых, закон и сертификация соответствия должны быть адаптированы таким образом, чтобы оригинальные производители оборудования, поставщики, а также все другие заинтересованные стороны в автомобильной промышленности могли согласовывать свои технологические разработки с четкими и стабильными требованиями к автоматизированным транспортным средствам.

В России, когда в управление транспортным средством в той или иной степени вовлечен водитель, действуют имеющиеся нормы УК РФ. Иное дело — при полной автономизации транспортного средства. Решение вопросов уголовной ответственности в этом случае представляет особую сложность по ряду причин. Во-первых, норма должна быть бланкетной по определению, однако на сегодняшний день правила, на которые надо будет ссылаться в уголовном законе, отсутствуют. Во-вторых, следует решить, что лежит в основе этиологии дорожно-транспортного происшествия при использовании высокоавтоматизированного транспортного средства: нарушение функционирования системы или нарушение правил

⁹ См.: Ethics Commission. Automated and Connected Driving. Report. June 2017 // URL: https://www.bmvi.de/SharedDocs/EN/publications/report-ethics-commission.pdf?__blob=publicationFile (дата обращения: 22.04.2019).

Таблица 1

Уровни автоматизации вождения (SAE J3016)

SAE J3016 УРОВНИ АВТОМАТИЗАЦИИ ВОЖДЕНИЯ						
	УРОВЕНЬ 0	УРОВЕНЬ 1	УРОВЕНЬ 2	УРОВЕНЬ 3	УРОВЕНЬ 4	УРОВЕНЬ 5
Что должен делать водитель?	Вы ведёте автомобиль, даже если ноги находятся не на педали, а руки не на руле			Вы не ведёте автомобиль, если активированы функции автоматического вождения		
	Вы обязаны следить за электронными ассистентами и подруливать, разгоняться и тормозить при необходимости			Если система попросит, вы должны взять управление на себя	Электронные ассистенты не требуют от человека брать управление на себя	
	Системы помощи водителю			Системы беспилотного вождения		
Что делает автоматика?	Ассистенты лишь предупреждают и оказывают кратковременную помощь	Ассистенты помогают рулить ИЛИ ускоряться/тормозить	Ассистенты помогают рулить И ускоряться/тормозить	Система может самостоятельно вести автомобиль только при одновременном выполнении нескольких условий		Система может самостоятельно вести автомобиль при любых условиях
Примеры систем	<ul style="list-style-type: none"> Автоматическое экстренное торможение; Предупреждение о слепых зонах; Предупреждение о покидании полосы 	<ul style="list-style-type: none"> Удержание в полосе ИЛИ Адаптивный круиз-контроль 	<ul style="list-style-type: none"> Удержание в полосе И Адаптивный круиз-контроль одновременно 	<ul style="list-style-type: none"> Ассистент движения в дорожных заторах 	<ul style="list-style-type: none"> Местное беспилотное такси; У автомобиля может не быть руля и педалей 	<ul style="list-style-type: none"> То же самое, что уровень 4, но способность автономного передвижения сохраняется везде



Рис. 1. Концептуальная схема распределения ответственности за причинение ущерба высокоавтоматизированным транспортным средством в зависимости от уровня автоматизации

дорожного движения как таковых (возможна совокупность указанных факторов). Это необходимо для определения правовой природы возможного преступления: транспортного или какого-то иного (например, технологического), а значит, определения объекта преступления и места последнего в системе Особенной части УК РФ. Нет ясности и в отношении субъекта ответственности: таковым должен являться эксплуатант, разработчик системы или производитель?

Кроме того, необходимо решить вопрос об ответственности за внешнее вмешательство в функционирование беспилотника; очевидно, что ни одна из норм УК РФ не охватывает подобные действия.

Таким образом, появление беспилотных транспортных средств и, как следствие, новых угроз безопасности личности требует адекватного отражения в системе законодательства России.

Следующим шагом в нормативном правовом регулировании эксплуатации высокоавтоматизированных транспортных средств вслед за постановлением Правительства РФ от 26 ноября 2018 г. № 1415 должны стать разработка и принятие соответствующего федерального закона примерно со следующей структурой:

Федеральный закон

«О регулировании использования транспортных средств, оборудованных системой автоматического управления, на территории Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации»

Статья 1. Сфера действия Федерального закона.

Статья 2. Цели и принципы.

Статья 3. Основные понятия.

Статья 4. Правовые основы.

Статья 5. Полномочия органов государственной власти Российской Федерации.

Статья 6. Требования к транспортным средствам, оборудованным системой автоматического управления.

Статья 7. Общие требования к использованию транспортных средств, оборудованных системой автоматического управления (сфера использования таких транспортных средств, этапы их внедрения).

Статья 8. Требования к автомобильным дорогам общего пользования (сертификация таких дорог в целях использования транспортных средств, оборудованных системой автоматического управления).

Статья 9. Федеральный государственный контроль в сфере использования транспортных средств, оборудованных системой автоматического управления.

Статья 10. О внесении изменений в Федеральный закон «О безопасности дорожного движения».

Статья 11. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях.

Статья 12. О внесении изменений в Федеральный закон «Об автомобильных дорогах и о дорожной деятельности в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации».

Статья 13. О внесении изменений в Федеральный закон «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля».

Статья 14. Переходные положения.

Статья 15. Порядок вступления в силу Федерального закона.

Принятие подобного рода федерального закона целесообразно по крайней мере по двум обстоятельствам: во-первых, он устранил пробельность в регулировании эксплуатации беспилотных транспортных средств; во-вторых, обеспечит дополнительную гарантию безопасности личности.

БИБЛИОГРАФИЯ

1. Коробеев А. И., Чучаев А. И. Беспилотные транспортные средства: новые вызовы общественной безопасности // Lex Russica. — 2019. — № 2.
2. Штаге Д. Автоматизированное вождение и спорные ситуации // Уголовное право: стратегия развития в XXI веке : материалы XVI Международной научно-практической конференции. — М., 2019.

Материал поступил в редакцию 6 мая 2019 г.

RESPONSIBILITY FOR CAUSING HARM BY A HIGHLY AUTOMATED VEHICLE: STATE AND PERSPECTIVES¹⁰

CHUCHAEV Aleksandr Ivanovich, Doctor of Law, Professor, Professor of the Department of Criminal Law of the Kutafin Moscow State Law University (MSAL)
moksha1@rambler.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

MALIKOV Sergey Vladimirovich, PhD in Law, Senior Lecturer of the Department of Criminal Law of the Kutafin Moscow State University of Law (MSAL)
s.v.malikov@yandex.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

Abstract. *The paper describes the existing in Russia regulatory legal responsibility for causing harm by a highly automated (unmanned) vehicle (BTS). The most significant documents currently include: Convention on Road Traffic; Road Safety Strategy in the Russian Federation; «Roadmap» to improve legislation and eliminate administrative barriers in order to ensure the implementation of the National Technology Initiative for the «Avtonet». The main attention is given to the order of the Government of the Russian Federation, in which the first approaches to the regulation of the operation of highly automated vehicles are indicated, the actors responsible for the case of damage by the drone are highlighted. The principles of the functioning of the BTS and the degree of their autonomy are shown in general terms. The authors analyze the approaches in the domestic criminal law to the responsibility of persons managing BTS and the approaches developed in foreign countries in relation to the regulation of the operation of highly automated vehicles. The main approaches to the definition of a criminal law prohibition are indicated and the most important algorithms of criminalization of the considered act are highlighted. The structure of the federal law on the regulation of the use of vehicles equipped with an automatic control system in the territory of the Russian Federation is proposed.*

Keywords: *unmanned vehicles (BTS), traffic crimes, legal regulation, crime, legal nature, criminalization, criminal liability, subject of crime, injury, draft law.*

REFERENCES (TRANSLITERATION)

1. Korobeev A. I., Chuchaev A. I. Bepilotnye transportnye sredstva: novye vyzovy obshchestvennoj bezopasnosti // Lex Russica. — 2019. — № 2.
2. Shtage D. Avtomatizirovannoe vozhdenie i spornye situacii // Ugolovnoe pravo: strategiya razvitiya v XXI veke : materialy XVI Mezhdunarodnoj nauchno-prakticheskoy konferencii. — M., 2019.

¹⁰ The study is carried out with the financial support of the Russian Foundation for Basic Research, Research Project No. 18-29-16162.

Использование цифровых технологий при допросе свидетелей на досудебных стадиях уголовного судопроизводства (сравнительно-правовой анализ законодательства Российской Федерации и законодательства некоторых иностранных государств)¹

***Аннотация.** Показания свидетелей представляют такой вид доказательств, без которых не обходится практически ни одно уголовное дело. Именно значение этого вида доказательств обуславливает законодательные требования к регламентации подготовки и процедуре допроса свидетеля, а также к фиксации показаний. Это приобретает особое значение как с позиции обеспечения гарантии допустимости и достоверности доказательства, так и с точки зрения обеспечения прав и законных интересов лиц, вовлеченных в уголовное судопроизводство.*

Национальное законодательство современных государств создает собственные стандарты использования показаний свидетеля в доказывании по уголовным делам. При всем многообразии подходов значение информационных технологий при собирании, проверке и оценке показаний свидетеля можно рассматривать по следующим основным направлениям: как средство фиксации следственного действия, как способ установления фактических обстоятельств, имеющих значение для дела, как средство обеспечения производства следственного действия и как средство передачи информации.

В работе на основе анализа уголовно-процессуального законодательства Российской Федерации и некоторых иностранных государств исследуются проблемы законодательного регулирования использования цифровых технологий при допросе свидетелей, в том числе дистанционный допрос и депонирование показаний свидетеля. Отдельное внимание уделено дистанционному допросу по запросу иностранных государств.

Ключевые слова: уголовное судопроизводство, досудебные стадии, свидетели, показания свидетелей, допрос свидетелей, цифровые технологии, цифровизация, дистанционный допрос, депонирование показаний, доказательства.

¹ Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16041.

© Антонович Е. К., 2019

* Антонович Елена Константиновна, кандидат юридических наук, доцент кафедры уголовно-процессуального права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), полковник внутренней службы в отставке
e.ant@inbox.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

DOI: 10.17803/1994-1471.2019.103.6.125-136

Еще недавно цифровые технологии использовались исключительно в вычислительной цифровой электронике, в компьютерах, в различных сферах электротехники, таких как робототехника, автоматизация, радио- и телекоммуникационные устройства. Но цифровые технологии уверенно входят в нашу жизнь. Сохранение и предоставление информации в необходимом виде и объеме, передача информации посредством цифровых технологий на большие расстояния — все это находит применение во многих отраслях. И вот уже достаточно активно исследуются проблемные вопросы, касающиеся использования электронной информации в доказывании и электронных доказательствах в уголовном судопроизводстве².

Хотя уголовное дело в электронном формате уже и не кажется чем-то фантастическим в связи с провозглашением такой возможности в законодательстве некоторых иностранных государств, дискуссии относительно цифровизации российского уголовного судопроизводства не утихают.

Несмотря на наличие в юридической литературе различных подходов к пониманию цифровизации, цифровизацию в уголовном судопроизводстве следует рассматривать как обусловленный стремлением повысить эффективность уголовного судопроизводства и гарантировать защиту прав и свобод лиц, вовлеченных в уголовное судопроизводство, способ использования на единой цифровой платформе инфор-

мационных технологий в парадигме принятия решений и доказывания в уголовном судопроизводстве. Именно с этих позиций нами рассматриваются проблемы использования цифровых технологий при допросе свидетелей на досудебных стадиях уголовного судопроизводства и связанные с этим вопросы совершенствования уголовно-процессуального законодательства.

В юридической литературе следственные действия рассматриваются в двух аспектах — познавательном и процессуальном³. Показания свидетелей — такой вид доказательств, без которых вряд ли обходится рассмотрение уголовного дела. В этой связи регламентация подготовки и процедуры допроса свидетеля и фиксации показаний приобретает особое значение как с точки зрения гарантии допустимости и достоверности доказательства, так и с точки зрения обеспечения прав и законных интересов лиц, вовлеченных в уголовное судопроизводство.

В стремлении максимально использовать возможности развивающихся информационных процессов национальное законодательство современных государств создает свои стандарты их использования в доказывании по уголовным делам. При всем многообразии подходов значение информационных технологий при собирании, проверке и оценке показаний свидетеля можно рассматривать по следующим основным направлениям: как средство фиксации следственного действия, как способ установления фактических обстоятельств, имеющих значение

² См., например: *Пастухов П. С.* Проблемы законодательного регулирования использования электронной информации в качестве доказательств по уголовному делу // Черные дыры в российском законодательстве. 2015. № 3. С. 127—130; *Васюков В. Ф.* Осмотр, выемка электронных сообщений и получение компьютерной информации // Уголовный процесс. 2016. № 10. С. 64—67; *Вехов В. Б.* Понятие, виды и особенности фиксации электронных доказательств // Расследование преступлений: проблемы и пути их решения. 2016. № 1. С. 155—158; *Бессмертная А. И.* Проблемы и перспективы использования электронных доказательств в уголовном процессе // Обеспечение прав и свобод человека в уголовном судопроизводстве: организационные, процессуальные и криминалистические аспекты : сборник статей по материалам междунар. студ. науч.-практ. конференции. Новосибирск, 2017. С. 32—35; *Стельмах В. Ю.* Электронная информация в доказывании по уголовным делам: способы получения и место в системе доказательств // Библиотека криминалиста. Научный журнал. 2018. № 3. С. 93—100.

³ См. подробнее: *Шейфер С. А.* Следственные действия: система и процессуальная форма. М. : Юрлитинформ, 2001. С. 5—38, 39—50.

для дела, как средство обеспечения производства следственного действия и как средство передачи информации.

В Российской Федерации вызов и допрос свидетелей осуществляются в порядке, установленном ст. 187—191 Уголовно-процессуального кодекса Российской Федерации.

В соответствии с ч. 4 ст. 189 УПК РФ в ходе допроса по инициативе следователя или по ходатайству допрашиваемого лица могут быть проведены фотографирование, аудио- и (или) видеозапись, киносъемка, материалы которых хранятся при уголовном деле и по окончании предварительного следствия опечатываются. В этом случае согласно ч. 4 ст. 190 УПК РФ в протоколе допроса делается соответствующая отметка с указанием сведений о технических средствах, об условиях фотографирования, аудио- и (или) видеозаписи, киносъемки и о факте приостановления аудио- и (или) видеозаписи, киносъемки, о причине и длительности остановки их записи и заявления допрашиваемого лица по поводу проведения фотографирования, аудио- и (или) видеозаписи, киносъемки.

Законодательство иностранных государств также допускает возможность использования информационных технологий как средства фиксации и хранения юридически значимой информации. Например, в соответствии со ст. 148 УПК Эстонской Республики⁴ в случае необходимости доказательственная информация, помимо протокола, может быть зафиксирована в фото- или киноматериалах, звуко- или видеозаписях либо в иной наглядной форме. Фотоматериалы и иной наглядный материал приобщаются вместе с протоколом к материалам уголовного дела, а киноленты, звуко- и видеозаписи хранятся в упакованном виде при уголовном деле. Подробнее порядок фиксации и хранения этих материалов регламентируется в ст. 149—151 УПК Эстонской Республики. Согласно ч. 3 ст. 149 УПК Эстонской Республики цифровая фотография приводится в протоколе процессуального

действия или в качестве приложения к нему, хранится в виде компьютерного файла в системе электронного дела E-toimik. Цифровая фотография может быть изготовлена из отдельных кадров видеозаписи. При этом, обеспечивая достоверность доказательств, законодатель предусмотрел гарантии недопущения внесения изменений в фото-, кино-, звуко- или видеозаписи.

Отдельного рассмотрения заслуживает вопрос о допросе несовершеннолетних свидетелей.

Изложенная в редакции Федерального закона от 28 декабря 2013 г. № 432-ФЗ⁵ статья 191 УПК РФ возлагает на следователя и дознавателя, в отличие от допроса совершеннолетнего свидетеля, не право, а обязанность применять видеозапись или киносъемку в ходе допроса свидетеля. Исключением из этого являются ситуации, когда несовершеннолетний свидетель либо его законный представитель против этого возражают. Материалы видеозаписи или киносъемки хранятся при уголовном деле, а согласно ст. 281 УПК РФ видеозапись может быть воспроизведена в ходе судебного разбирательства. Аналогичный подход в части регламентации допроса несовершеннолетних и применения информационных технологий в ходе его проведения свойственен национальному законодательству других государств.

В ходе самого допроса свидетеля полученные ранее при помощи информационных технологий сведения могут быть использованы как лицом, производящим допрос, так и допрашиваемым лицом. Это позволяет расширить объем устанавливаемых сведений и обеспечить их достоверность.

Так, в соответствии с ч. 3 ст. 190 УПК РФ в ходе допроса допрашиваемому лицу следователем могут воспроизводиться материалы аудио- и (или) видеозаписи, киносъемки следственных действий, о чем делается запись в протоколе допроса. Законодательство иностранных государств также допускает такую возможность

⁴ URL: <https://v1.juristaitab.ee/ru/zakonodatelstvo/ugolovno-processualnyy-kodeks>(дата обращения: 8 февраля 2019 г.).

⁵ СПС «КонсультантПлюс».

(например, ч. 5 ст. 210 УПК Республики Казахстан⁶).

Но и допрашиваемое лицо при допросе в ходе предварительного расследования вправе пользоваться документами и записями (ч. 3 ст. 188 УПК РФ). Аналогичная норма предусмотрена ст. 279 УПК РФ, регламентирующей порядок использования свидетелем уже в ходе судебного следствия письменных заметок и документов. Эти документы предъявляются суду и могут быть приобщены к материалам уголовного дела.

Законодательство иностранных государств, допуская возможность допрашиваемого лица пользоваться документами и записями, акцентирует внимание на случаи, когда показания свидетеля связаны с цифровыми данными, трудно удерживаемыми в памяти (например, ч. 5 ст. 210 УПК Республики Казахстан; ч. 3 ст. 68 УПК Эстонской Республики).

Российский законодатель не дает ответа на вопрос, могут ли использоваться в данном случае записи лишь на бумажном носителе или допустимо использование записей при помощи цифровых технологий. Этот вопрос не должен быть оставлен без внимания. Однако такие записи должны приобщаться к материалам уголовного дела в условиях, исключающих возможность их изменения.

Использование видеоконференцсвязи для допроса свидетеля в российском уголовно-процессуальном законодательстве предусмотрено лишь в ходе судебного разбирательства (ч. 4 ст. 240, ст. 278.1 УПК РФ).

Допрос при помощи современных средств связи допускает и законодательство ряда иностранных государств. В их числе Германия, Италия, Финляндия, Швеция, Эстония, Молдова, Казахстан. Такой допрос возможен в основном в ходе судебного разбирательства, причем не только в ходе судебного следствия, но и при подготовке дела к судебному заседанию (в том

числе по телефону, как это предусмотрено ст. 2 УПК Финляндской Республики⁷).

Однако проблема дистанционного допроса актуальна и в ходе досудебного производства. Ведь свидетель, в том числе очевидец произошедшего, может на время или постоянно покинуть населенный пункт, в котором происходит предварительное расследование, в связи с длительной командировкой, отпуском, переездом и т.д. Вызов таких участников уголовного судопроизводства для проведения допроса требует финансовых затрат и дополнительного времени, что не может не сказываться негативно на эффективности расследования. Конечно, при производстве предварительного следствия следователь может, руководствуясь положениями ч. 1 ст. 152 УПК РФ, поручить производство допроса другому следователю или органу дознания. Однако показания этих свидетелей обычно необходимы в более сжатые сроки, чем предусмотренный законом 10-дневный срок.

Учитывая указанную актуальность, на рассмотрение в Государственную Думу Федерального Собрания РФ внесен проект федерального закона № 434998-7⁸, направленный на дополнение УПК РФ новой статьей 189.1, предусматривающей особенности допроса свидетеля по уголовному делу посредством видеоконференцсвязи.

Согласно законопроекту производство дистанционного допроса — право, а не обязанность следователя. Следователь сможет воспользоваться этим правом, либо вызвать на допрос свидетеля, либо направить поручение о его допросе. В месте нахождения свидетеля на следователя возлагается обязанность составить протокол, ознакомить с ним свидетеля и предъявить его для подписания. В протоколе планируется указывать лицо, составившее протокол, и всех участвующих лиц. По замыслу разработчиков законопроекта, следователь в месте нахождения свидетеля — это лицо, составившее и огласив-

⁶ URL: https://online.zakon.kz/Document/?doc_id=31575852 (дата обращения: 8 февраля 2019 г.).

⁷ URL: <https://www.legislationline.org/documents/section/criminal-codes/country/32/Finland/show> (дата обращения: 8 февраля 2019 г.).

⁸ Сайт Государственной Думы Федерального Собрания РФ. URL: <https://www.duma.gov.ru> (дата обращения: 8 февраля 2019 г.).

шее протокол, а следователь, в производстве которого находится уголовное дело, — лицо, допросившее свидетеля, который также подписывает протокол после его получения. В остальном допрос посредством видеоконференцсвязи проводится по правилам ст. 189 УПК РФ. Такой допрос предлагается проводить и в отношении несовершеннолетних.

С учетом развития цифровых технологий рассмотренный законопроект не лишен недостатков. Его доработка могла бы строиться по следующим основным направлениям: создание процессуальных оснований проведения дистанционного допроса; укрепление процессуального статуса его участников; уточнение процедуры его проведения и фиксации результатов следственного действия; определение порядка передачи результатов следственного действия по месту производства предварительного расследования.

Так, основания для производства дистанционного допроса, согласно законопроекту, — невозможность личного участия свидетеля в производстве по уголовному делу. Однако разработчики не раскрывают конкретные случаи, когда участие свидетеля невозможно, не излагают перечень субъектов, по чьей инициативе возможен такой допрос.

Обратимся к законодательному опыту некоторых иностранных государств.

Например, в УПК Республики Молдова⁹ особое внимание уделено использованию телеконференцсвязи для дистанционного допроса в целях обеспечения безопасности свидетеля. Предусмотрено право свидетеля быть информированным о возможности допроса посредством телеконференции с изменением внешности и голоса (ч. 12 ст. 90 УПК Республики Молдова). Вместе с тем согласно ст. 110 УПК Республики Молдова основанием допроса свидетеля не по месту нахождения органа уголовного преследования, а посредством технических средств являются не только основания полагать, что жизнь, телесная неприкосновенность или свобода сви-

детеля или его близкого родственника находятся в опасности в связи с данными им показаниями по делу о тяжком, об особо тяжком или о чрезвычайно тяжком преступлении, но и наличие соответствующих технических средств. Такому свидетелю разрешается сообщить иную, чем это есть на самом деле, информацию о своей личности. Подлинная информация о его личности вносится в отдельный протокол и хранится в запечатанном конверте с соблюдением секретности. Свидетель может быть допрошен посредством закрытой телеконференции с таким изменением внешности и голоса, чтобы его невозможно было узнать, однако обвиняемому, его защитнику и потерпевшему обеспечивается возможность задавать ему вопросы.

Согласно ст. 69 УПК Эстонской Республики лицо, ведущее производство, может провести дистанционный допрос свидетеля в следующих случаях: непосредственный допрос свидетеля затруднен, непосредственный допрос свидетеля повлечет за собой чрезмерные затраты, необходима защита свидетеля.

Аналогичный подход заложен в уголовно-процессуальном законодательстве Швеции (ст. 144 УПК Швеции¹⁰), причем допускается производство допроса путем видеоконференции как государственным обвинителем, так и судом.

УПК Республики Казахстан в ст. 213 предусмотрен более широкий спектр оснований для производства дистанционного допроса. Помимо затруднений или невозможности прибытия, финансовыми затратами и необходимостью обеспечения безопасности лиц, отдельно выделены еще три основания: допрос несовершеннолетних свидетелей и потерпевших; обеспечение соблюдения сроков досудебного расследования; наличие причин, дающих основания полагать, что допрос будет затруднен или связан с излишними затратами.

В рассматриваемом законопроекте также следовало бы детализировать основания производства дистанционного допроса, в том числе указав следующие случаи:

⁹ URL: http://online.zakon.kz/Document/?doc_id=30397729#pos=6;-155 (дата обращения: 8 февраля 2019 г.).

¹⁰ URL: <https://www.admin.ch/opc/en/classified-compilation/20052319/index.html> (дата обращения: 8 февраля 2019 г.).

- личное присутствие допрашиваемого лица невозможно (из-за состояния здоровья, возраста, наличия малолетних детей и членов семьи, нуждающихся в постоянном уходе, иных уважительных причин);
- личное присутствие допрашиваемого лица возможно, но связано с неоправданными расходами, например в связи с длительными командировками за пределами субъекта, в котором проводится предварительное расследование;
- в отношении свидетелей, к которым применяются меры безопасности (в ч. 9 ст. 160 УПК РФ регламентируется процедура допроса так называемого анонимного свидетеля, в отношении которого принимаются меры безопасности, между тем соответствующее отражение в рассматриваемом законопроекте отсутствует, хотя могло бы обеспечить дополнительные гарантии соблюдения прав и законных интересов участников уголовного судопроизводства, сократить сроки предварительного расследования и финансовые расходы, гарантируя достоверность доказательств);
- проведение допроса несовершеннолетнего свидетеля (как уже отмечалось, на сегодняшний день российское уголовно-процессуальное законодательство предусматривает возможность фиксации такого допроса при помощи информационных технологий, но не предусматривает возможности производства дистанционного допроса);
- наличие иных причин, дающих основания полагать, что допрос будет затруднен.

Интересно решен вопрос об инициаторе дистанционного допроса в уголовно-процессуальном законодательстве Республики Казахстан. В отличие от УПК Эстонской Республики, в соответствии с ч. 2 ст. 213 УПК Республики Казахстан лицо, осуществляющее расследование дела, принимает решение о производстве дистанционного допроса не только по собственной инициативе, но и по ходатайству стороны или других участников уголовного процесса либо по указанию прокурора.

В рассматриваемом законопроекте лишь указано, что проведение такого допроса возможно

на основании постановления следователя. Инициатива его проведения не должна исходить исключительно от следователя или дознавателя. Ведь именно свидетель, как никто иной, может проявить такую заинтересованность. В то время как проверку соответствующего ходатайства, установление основания при наличии соответствующего повода и принятие решения о необходимости такого допроса следует возложить на должностное лицо.

Анализ законодательства иностранных государств позволяет выделить разновидности дистанционного допроса в зависимости от вида информационных технологий, используемых в качестве способа его проведения: допрос при помощи технического решения, в результате чего участники процесса непосредственно видят и слышат в прямой трансляции показания свидетеля, не находящегося в следственном органе, и могут задавать ему вопросы через лицо, ведущее производство; допрос по телефону, в результате чего участники процесса непосредственно слышат показания свидетеля, не находящегося в следственном органе, и могут задавать ему вопросы через лицо, ведущее производство (например, ст. 69 УПК Эстонской Республики).

Допрос по телефону занимает достаточно уверенное положение в законодательстве многих зарубежных государств. Конечно, восприятие информации по телефону нельзя сравнить с непосредственным наблюдением за лицом, которое дает показания, пусть даже при помощи видеоконференцсвязи. Однако соотношение отсутствия показаний или их наличия позволяет усомниться в категоричном отрицании такой возможности. К тому же, как и любые другие доказательства, эти доказательства должны подвергаться проверке и оценке в порядке, предусмотренном уголовно-процессуальным законодательством.

Необходимо уточнить процедуру допроса.

Так, остается открытым вопрос о возможности формулировать или уточнять вопросы в ходе этого следственного действия следователями по месту производства предварительного расследования и по месту производства допроса.

Не решен вопрос технического обеспечения проведения этого допроса. В частности, обо-

рудования помещений, в котором проводится допрос и в котором допрос транслируется, а также необходимости проведения таких допросов на единой цифровой платформе. Должны быть определенные гарантии того, что использование цифровых технологий не исказит информацию.

Например, в ч. 2 ст. 213 УПК Республики Казахстан провозглашено, что использование при дистанционном допросе научно-технических средств и технологий должно обеспечивать надлежащее качество изображения и звука, а также информационную безопасность. А согласно ст. 115 УПК Республики Молдова не допускается аудио- или видеозапись только какой-то части допроса, а также специальное повторение для производства аудио- или видеозаписи ранее данных показаний.

Использование при дистанционном допросе научно-технических средств и цифровых технологий должно обеспечивать высокое качество изображения и звука, а также информационную безопасность. В этой связи нельзя исключать участие сведущего лица в этой области при подготовке и производстве такого допроса. Следовательно, круг лиц, принимающих участие в дистанционном допросе, может быть значительно шире, чем при обычном допросе в месте производства предварительного расследования.

Отсутствует регламентация участия в допросе других участников уголовного судопроизводства, в частности адвоката, специалиста, законных представителей, переводчиков, педагогов и психологов. Авторам законопроекта стоило бы попытаться разрешить вопрос о том, могут ли (должны ли) находиться эти участники уголовного судопроизводства в месте непосредственного допроса или в месте трансляции дистанционного допроса. Этим участникам должно быть предоставлено право заявлять отводы не только следователю, но и специалисту, технически обеспечивающему допрос, а также другие права.

В ходе производства по уголовному делу может возникнуть необходимость допроса также потерпевшего, эксперта, специалистов, других участников уголовного судопроизводства. В этой

связи процессуальные гарантии дистанционного допроса могли бы быть распространены и на других участников уголовного судопроизводства.

Согласно законопроекту, как и по законодательству иностранных государств, результат такого дистанционного допроса оформляется протоколом¹¹. Законодательство некоторых иностранных государств акцентирует внимание на том, что после проведения аудио- или видеозаписи допроса сделанная таким образом запись должна быть переписана как можно скорее после завершения допроса. После того как копия оригинальной пленки сделана для целей составления стенограммы, оригинал ленты или один из оригиналов должен быть опечатан и заверен соответствующими подписями (например, ст. 79 УПК Боснии и Герцеговины¹²).

Авторами законопроекта не предусмотрен механизм передачи протокола, составленного по итогам дистанционного допроса. Таким образом, законопроект, нацеленный на сокращение сроков производства по делу, по сути, не исключает увеличения этих сроков. Между тем современные информационные технологии могли бы быть использованы и в этом случае.

Производство допроса свидетелей не исключает необходимости проведения очной ставки между ними либо между ними и другими участниками уголовного судопроизводства. Так, ч. 6 ст. 77 УПК Эстонской Республики позволяет организовать очную ставку при помощи технических средств, однако не предусматривает механизма производства дистанционной очной ставки.

Следовало бы отдельно продумать особенности дистанционного допроса несовершеннолетних свидетелей. Необходимость отрываться от привычной среды, преодолевать большие расстояния для дачи показаний не может не сказаться негативно на подростке. В то же время допрос хотя и в следственном подразделении, но вблизи от дома позволит максимально смягчить указанные моменты. Это касается не только процедуры допроса, но и особенностей оборудования комнаты, в которой будет проводиться

¹¹ См., например: УПК Эстонской Республики, УПК Республики Казахстан.

¹² URL: www.ohr.int/ohr-dept/.../criminal-procedure-code-of-bih.do (дата обращения: 8 февраля 2019 г.).

дистанционный допрос. Так, например, в УПК Республики Молдова предусмотрена норма, раскрывающая понятие «допросная комната» применительно к допросу несовершеннолетнего пострадавшего и свидетеля (п. 4.1 ст. 6).

И наконец, нельзя забывать о других следственных действиях, возможность проведения которых дистанционно также должна быть рассмотрена. Например, опознание или выемка, обыск и т.д.

В условиях развития цифровых технологий вопрос о депонировании показаний свидетеля, обусловленный стремлением обеспечить некий баланс публичных и частных интересов в уголовном судопроизводстве, представляется также небезынтесным.

Так, в Гонконге в отношении наиболее уязвимых свидетелей, которые могут стать жертвами преступления, обеспечивается защита, в том числе посредством предоставления возможности давать показания не только по прямой телетрансляции, но и посредством воспроизведения предварительно записанных видеодоказательств в электронном виде¹³.

В соответствии со ст. 109 УПК Республики Молдова основаниями депонирования показаний свидетелей являются следующие случаи: свидетель не сможет присутствовать при рассмотрении дела в суде по причине его выезда за границу; свидетель не сможет присутствовать при рассмотрении дела в суде по другим обоснованным причинам; сокращение или устранение угрозы явной опасности свидетелю; предупреждение ревиктимизации свидетеля. Правом требовать депонирования показаний наделяется прокурор, а подозреваемому, обвиняемому, его защитнику, потерпевшему обеспечивается возможность задать вопросы допрашиваемому свидетелю.

В статье 217 УПК Республики Казахстан содержится более широкий круг лиц, наделенный полномочиями инициировать такого рода допрос: прокурор, следователь, начальник органа дознания, подозреваемый или его адвокат, участвующий в деле в качестве защитника. А ос-

нованиями депонирования показаний свидетелей являются следующие случаи: основания полагать, что более поздний их допрос в ходе досудебного расследования либо судебного заседания может оказаться невозможным в силу объективных причин (постоянное проживание за пределами Республики Казахстан, выезд за границу, тяжелое состояние здоровья, применение мер безопасности); исключение последующих допросов несовершеннолетних свидетелей для исключения психотравмирующего воздействия.

В уголовно-процессуальном законодательстве ФРГ допрос при помощи информационных технологий вне основного места слушания также возможен (Ст. 58b УПК ФРГ¹⁴). А основаниями допроса свидетеля на аудиовизуальном носителе возможна являются случаи: интересы защиты несовершеннолетних, не достигших 18-летнего возраста; наличие опасности, что не удастся допросить свидетеля во время основного слушания, и запись необходима для установления истины; интересы несовершеннолетних потерпевших, в отношении которых совершены определенные преступления (ст. 58a УПК ФРГ). Предусматриваются и ограничения на использование таких депонированных показаний: они используются только для целей уголовного преследования. Копии записи могут быть предоставлены только лицам, имеющим право ознакомиться с файлами, не могут быть продублированы или переданы куда-либо. А файлы хранятся в прокуратуре (ст. 58a УПК ФРГ).

Таким образом, депонирование показаний свидетеля заключается в закреплении показаний свидетеля в том случае, когда имеются основания полагать, что его допрос в более поздний срок в ходе досудебного производства либо судебного следствия может оказаться невозможным ввиду объективных причин. Однако относить этот вид допроса к дистанционному допросу нельзя, поскольку допрашивающий и допрашиваемый находятся в одном помещении. Объединяет эти два вида допроса лишь способ фиксации показаний.

¹³ URL: <https://www.doj.gov.hk/eng/public/pubsoppapcon.html> (дата обращения: 8 февраля 2019 г.).

¹⁴ URL: <http://www.gesetze-im-internet.de/stpo/index.html> (дата обращения: 8 февраля 2019 г.).

При положительном решении о возможности включения депонирования показаний в УПК РФ потребуется формулирование отдельной статьи.

При оказании правовой помощи по уголовным делам доказывание имеет свою специфику. Это обусловлено трансграничным характером собирания доказательств с участием иностранных компетентных органов и должностных лиц, применением международного и иностранного законодательства в случаях, предусмотренных международными договорами или на основе принципа взаимности. Однако не всегда можно получать показания свидетеля и таким способом. В этой связи законодательство некоторых иностранных государств допускает возможность проведения дистанционного допроса свидетеля, находящегося за пределами территории государства.

Так, в соответствии с ч. 5 ст. 205-ter УПК Итальянской Республики¹⁵ участие свидетеля в слушании через аудиовизуальное соединение происходит в соответствии с условиями, предусмотренными международными соглашениями о судебном разбирательстве. Данная норма хотя и касается дистанционного допроса свидетеля в ходе судебного разбирательства, однако представляет интерес с точки зрения допустимости таких дистанционных показаний свидетеля в уголовном судопроизводстве.

Статья 468 УПК Эстонской Республики посвящена регламентации дистанционного допроса лица, находящегося в иностранном государстве, на основе соответствующего ходатайства и при согласии свидетеля на проведение этого допроса. Ограничения на допрос по телефону содержатся лишь в отношении подозреваемого и обвиняемого, а в отношении свидетеля аналогичных изъятий в законе не предусмотрено. Достаточно подробно регламентирована сама процедура такого допроса. Им руководит представитель компетентного правового органа ходатайствующего государства в соответствии с процессуальным законом своего государства. При вызове на дистанционный допрос предписано руководствоваться процессуальным законом

исполняющего государства. Допрашиваемый может отказаться от дачи показаний также на основании процессуального закона исполняющего государства. Компетентный правовой орган исполняющего государства, организующий дистанционный допрос, назначает и сообщает время проведения дистанционного допроса; обеспечивает вызов допрашиваемого и его явку на допрос; несет ответственность за установление личности допрашиваемого и за исполнение законов своего государства; в случае необходимости обеспечивает участие переводчика. Запись дистанционного допроса ведет компетентный правовой орган ходатайствующего государства, но дополнительную запись может также вести и компетентный правовой орган исполняющего государства. Протокол аудиовизуального дистанционного допроса составляет компетентный правовой орган исполняющего государства, а в случае допроса по телефону — компетентный правовой орган ходатайствующего государства. К содержанию протокола предъявляются определенные требования.

Статья 576 УПК Республики Казахстан содержит не только регламентацию процессуальных действий по запросу компетентного органа иностранного государства, но и его основания: невозможность прибытия вызываемых лиц в компетентный орган иностранного государства; обеспечение безопасности лиц; иные основания, предусмотренные международным договором. Процессуальные действия путем видеосвязи выполняются в порядке, предусмотренном процессуальным законом запрашивающей стороны в той мере, в которой такой порядок не противоречит принципам уголовно-процессуального законодательства Республики Казахстан. Обязанность обеспечить участие переводчика при проведении видеосвязи возложена на компетентный орган запрашивающей стороны. Протокол и носители видеoinформации направляются в компетентный орган запрашивающей стороны. Аналогичным образом проводятся процессуальные действия с помощью видеосвязи по запросам компетентного органа Республики Казахстан.

¹⁵ URL: <https://lexscripta.it/codici/disp-att-cpp> (дата обращения: 8 февраля 2019 г.).

Законодательный опыт иностранных государств, касающийся создания правовой основы для дистанционного допроса, проводимого в рамках международного сотрудничества, может быть полезен при проработке этого вопроса относительно возможности введения соответствующей нормы в российское уголовно-процессуальное законодательство. Для создания правовых основ проведения допроса свидетеля, потерпевшего, иных участников уголовного судопроизводства необходимо выработать позицию по следующим вопросам: определение круга лиц, в отношении которых производство дистанционного допроса допустимо; формирование процедуры производства дистанционного допроса; установление круга участников уголовного судопроизводства, участвующих в его подготовке и проведении, и законодательное закрепление их прав и обязанностей в этой связи (в том числе касающихся возможности заявления отводов); выработка механизма фиксации результатов такого следственного действия, проведенного при помощи современных информационных технологий; определение требований к самим информационным технологиям и их соблюдение; выявление критериев допустимости и достоверности доказательств, полученных в результате этого следственного действия.

Нами уже рассматривались критерии допустимости доказательств, полученных за пределами территории Российской Федерации¹⁶. Представляется, что все они могут быть применены и к дистанционному допросу в рамках оказания правовой помощи по уголовным делам, с тем лишь отличием, что представитель запрашивающей стороны сможет дистанционно присутствовать при производстве следственного действия и не только получать информа-

цию на заранее подготовленные вопросы, но и формулировать их по ходу следственного действия. Участие этого представителя, а также переводчика и иных лиц, их полномочия должны быть оговорены в поручении, содержащемся в запросе о правовой помощи, которое рассматривается как основание для международного сотрудничества¹⁷. В соответствии с положениями международных договоров и ст. 454 УПК РФ форма составления запроса — письменная. Передача запроса в устной форме с последующим подтверждением его в письменной форме возможна в случаях, предусмотренных международными договорами¹⁸. Однако в условиях развития информационных технологий передача такого запроса могла бы происходить и с их помощью.

Использование дистанционного допроса свидетеля в рамках оказания правовой помощи по уголовным делам позволит получать наиболее содержательные показания в более короткий срок, что в конечном итоге позволит повысить эффективность этого следственного действия. Но изучение этого вопроса должно быть обусловлено наличием соответствующей международной правовой базы.

Таким образом, вектор изменений российского уголовно-процессуального законодательства, регламентирующего производство допроса свидетелей на стадии предварительного расследования, должен быть направлен на максимально эффективное использование современных цифровых технологий. С одной стороны, необходимо учитывать положительный зарубежный опыт, а с другой — ориентироваться на исторически обусловленный собственный законодательный опыт, исключая переписывание вслепую под кальку чужих шаблонов.

¹⁶ См.: Антонович Е. К. К вопросу о допустимости доказательств, полученных за пределами территории Российской Федерации в рамках оказания правовой помощи по уголовным делам // Труды Академии управления МВД России. 2014. № 4. С. 41—44.

¹⁷ См.: Антонович Е. К. Запрос о правовой помощи, его значение и место в системе принятия решений в уголовном судопроизводстве // Юридическое образование и наука. 2017. № 5. С. 12—16.

¹⁸ См.: Антонович Е. К. Требования, предъявляемые к содержанию и форме запроса о производстве процессуальных действий, и последствия их несоблюдения // Международное публичное и частное право. 2016. № 5. С. 24—27.

БИБЛИОГРАФИЯ

1. Антонович Е. К. Запрос о правовой помощи, его значение и место в системе принятия решений в уголовном судопроизводстве // Юридическое образование и наука. — 2017. — № 5. — С. 12—16.
2. Антонович Е. К. К вопросу о допустимости доказательств, полученных за пределами территории Российской Федерации в рамках оказания правовой помощи по уголовным делам // Труды Академии управления МВД России. — 2014. — № 4. — С. 41—44.
3. Антонович Е. К. Требования, предъявляемые к содержанию и форме запроса о производстве процессуальных действий, и последствия их несоблюдения // Международное публичное и частное право. — 2016. — № 5. — С. 24—27.
4. Бессмертная А. И. Проблемы и перспективы использования электронных доказательств в уголовном процессе // Обеспечение прав и свобод человека в уголовном судопроизводстве: организационные, процессуальные и криминалистические аспекты : сборник статей по материалам международной студенческой научно-практической конференции. — Новосибирск, 2017. — С. 32—35.
5. Васюков В. Ф. Осмотр, выемка электронных сообщений и получение компьютерной информации // Уголовный процесс. — 2016. — № 10. — С. 64—67.
6. Вехов В. Б. Понятие, виды и особенности фиксации электронных доказательств // Расследование преступлений: проблемы и пути их решения. — 2016. — № 1. — С. 155—158.
7. Пастухов П. С. Проблемы законодательного регулирования использования электронной информации в качестве доказательств по уголовному делу // Черные дыры в российском законодательстве. — 2015. — № 3. — С. 127—130.
8. Стельмах В. Ю. Электронная информация в доказывании по уголовным делам: способы получения и место в системе доказательств // Библиотека криминалиста. Научный журнал. — 2018. — № 3. — С. 93—100.
9. Шейфер С. А. Следственные действия: система и процессуальная форма. — М. : Юрлитинформ, 2001. — С. 5—50.

Материал поступил в редакцию 6 мая 2019 г.

THE USE OF DIGITAL TECHNOLOGY IN THE INTERROGATION OF WITNESSES IN THE PRE-TRIAL STAGES OF CRIMINAL PROCEEDINGS (COMPARATIVE LEGAL ANALYSIS OF THE RUSSIAN FEDERATION LEGISLATION AND LAWS OF SOME FOREIGN COUNTRIES)¹⁹

ANTONOVICH Elena Konstantinovna, PhD in Law, Associate Professor of the Department of Criminal Procedure Law of the Kutafin Moscow State University (MSAL), Internal Service Colonel in Retirement
e.ant@inbox.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

Abstract. *The testimony of witnesses represents the type of evidence, without which practically no criminal case can do. It is the significance of this type of evidence that determines the legislative requirements for the regulation of preparation and the procedure for the interrogation of a witness, as well as for the recording of evidence. This is of particular importance both from the standpoint of ensuring the admissibility and reliability of evidence, as well as from the point of view of ensuring the rights and legitimate interests of persons involved in criminal proceedings.*

¹⁹ The study is carried out with the financial support of the Russian Foundation for Basic Research, Research Project No. 18-29-16041.

The national legislation of modern states creates its own standards for the use of witness testimony in proving criminal cases. With all the variety of approaches, the importance of information technology in the collection, testing and evaluation of witness testimony can be viewed in the following main areas: as a means of fixing an investigative action, as a way of establishing the actual circumstances relevant to the case, as a means of ensuring the production of an investigative action, and as a means of transmitting information.

Based on the analysis of the criminal procedure legislation of the Russian Federation and some foreign countries, the paper examines the problems of legislative regulation of the use of digital technologies during the interrogation of witnesses, including remote interrogation and deposition of witness testimony. Special attention is given to distant interrogation at the request of foreign countries.

Keywords: *criminal proceedings, pre-trial stages, witnesses, witness testimony, witness interrogation, digital technologies, digitalization, remote interrogation, deposition of testimony, evidence.*

REFERENCES (TRANSLITERATION)

1. Antonovich E. K. Zпрос o pravovoj pomoshchi, ego znachenie i mesto v sisteme prinyatiya reshenij v ugovnom sudoproizvodstve // Yuridicheskoe obrazovanie i nauka. — 2017. — № 5. — S. 12—16.
2. Antonovich E. K. K voprosu o dopustimosti dokazatel'stv, poluchennyh za predelami territorii Rossijskoj Federacii v ramkah okazaniya pravovoj pomoshchi po ugovnym delam // Trudy Akademii upravleniya MVD Rossii. — 2014. — № 4. — S. 41—44.
3. Antonovich E. K. Trebovaniya, predyavlyayemye k sodержaniyu i forme zaprosa o proizvodstve processual'nyh dejstvij, i posledstviya ih nesoblyudeniya // Mezhdunarodnoe publichnoe i chastnoe pravo. — 2016. — № 5. — S. 24—27.
4. Bessmertnaya A. I. Problemy i perspektivy ispol'zovaniya elektronnyh dokazatel'stv v ugovnom processe // Obespechenie prav i svobod cheloveka v ugovnom sudoproizvodstve: organizacionnye, processual'nye i kriminalisticheskie aspekty : sbornik statej po materialam mezhdunarodnoj studencheskoj nauchno-prakticheskoy konferencii. — Novosibirsk, 2017. — S. 32—35.
5. Vasyukov V. F. Osmotr, vyemka elektronnyh soobshchenij i poluchenie komp'yuternoj informacii // Ugovnyj process. — 2016. — № 10. — S. 64—67.
6. Vekhov V. B. Ponyatie, vidy i osobennosti fiksacii elektronnyh dokazatel'stv // Rassledovanie prestuplenij: problemy i puti ih resheniya. — 2016. — № 1. — S. 155—158.
7. Pastuhov P. S. Problemy zakonodatel'nogo regulirovaniya ispol'zovaniya elektronnoj informacii v kachestve dokazatel'stv po ugovnomu delu // Chernye dyry v rossijskom zakonodatel'stve. — 2015. — № 3. — S. 127—130.
8. Stel'mah V. Yu. Elektronnaya informaciya v dokazyvanii po ugovnym delam: sposoby polucheniya i mesto v sisteme dokazatel'stv // Biblioteka kriminalista. Nauchnyj zhurnal. — 2018. — № 3. — S. 93—100.
9. Shejfer S. A. Sledstvennye dejstviya: sistema i processual'naya forma. — M. : Yurlitinform, 2001. — S. 5—50.

Л. Н. Масленникова*

Трансформация досудебного производства в начальный этап уголовного судопроизводства, обеспечивающий доступ к правосудию в эру Industry 4.0¹

Аннотация. В статье рассматриваются актуальные проблемы обеспечения доступа к правосудию в уголовном судопроизводстве, обосновывается необходимость смены парадигмы досудебного производства. Новая цифровая реальность Industry 4.0 предполагает колоссальные темпы развития, глубинные изменения во всех сферах общества, в том числе в уголовном судопроизводстве. Автор утверждает, что цифровая трансформация уголовного судопроизводства в части обеспечения доступа к правосудию невозможна, если не изменить законодательную модель (алгоритм) начального этапа уголовного судопроизводства, обеспечивающего доступ к правосудию. Ключевым моментом в трансформации досудебного производства должно стать электронное взаимодействие государства и общества (населения) в новой цифровой реальности. Появляются принципиально новые возможности участия в уголовном судопроизводстве (в том числе удаленно) и новые возможности влияния на принятие решений и контроль за принятием решений (автоматизация регистрации сообщения о преступлении и начала расследования, возможность подачи жалоб, ходатайств, получение уведомлений, копий решений в электронном виде).

Ключевые слова: уголовное судопроизводство, начальный этап, доступ к правосудию, досудебное производство, цифровая трансформация, смена парадигмы, услуга государства, автоматизация регистрации сообщения о преступлении, электронное взаимодействие, электронный документ.

DOI: 10.17803/1994-1471.2019.103.6.137-146

Начало новой эры связывают с четвертой промышленной революцией, получившей условное название Industry 4.0, которая началась в конце XX в., базируется на современных цифровых технологиях и предполагает колос-

сальные темпы развития, глубинные изменения во всех сферах общества. Президент Всемирного экономического форума в Давосе К. Шваб выделил три блока мегатрендов четвертой промышленной революции: физический (беспилотные

¹ Публикация подготовлена в рамках проекта № 18-29-16018 «Концепция построения уголовного судопроизводства, обеспечивающего доступ к правосудию, в условиях развития цифровых технологий» при финансовой поддержке Российского фонда фундаментальных исследований.

© Масленникова Л. Н., 2019

* Масленникова Лариса Николаевна, доктор юридических наук, профессор, профессор кафедры уголовно-процессуального права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)

mIn1954@yandex.ru

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

транспортные средства, 3D-печать, передовая робототехника, новые материалы), цифровой (взаимодействие между благами и людьми на базе цифровых технологий) и биологический (синтетическая биология, биоинженерия)².

Благодаря новым цифровым технологиям прогнозируется переход на полностью цифровое производство, управляемое интеллектуальными системами в режиме реального времени в постоянном взаимодействии с внешней средой.

Отставание России в цифровой экономике (по мнению «Бостон Консалтинг Групп» (исследование 2016 г.), Россия находится на 39-м месте среди цифровых экономик мира), с точки зрения юристов, — это в первую очередь шанс избежать чужих ошибок³.

Современный этап развития информационных технологий ставит перед государственной властью непростую задачу: впервые ей приходится сталкиваться с огромным количеством технологий, которые противоречат сути государственного управления. Одной из таких технологий является блокчейн⁴. Централизованное государственное

управление и публично-правовая природа уголовного судопроизводства могут столкнуться с серьезными рисками при переходе на качественно новый уровень использования информационно-телекоммуникационных технологий.

Научные дискуссии в XXI в. в сфере уголовно-процессуального права и практики его применения в основном развернулись именно относительно благ и рисков внедрения современных цифровых технологий в организацию уголовно-процессуальной деятельности.

Ученые исследуют возможности применения технологии блокчейн для информатизации судебной системы⁵, оптимизацию судебного контроля на начальном этапе уголовного судопроизводства в условиях развития цифровых технологий⁶, особенности информационно-коммуникационного обеспечения уголовного судопроизводства РФ⁷, перспективы введения электронной формы уголовного дела⁸, электронное правосудие⁹; отличия в понимании сущности электронного правосудия в России и за рубежом¹⁰, вопросы доказывания и доказательств

² Шваб К. Четвертая промышленная революция. М. : Э, 2017. С. 27—37.

³ Быков А. Ю. Право цифровой экономики: некоторые народно-хозяйственные и политические риски. М. : Проспект, 2018. С. 20.

⁴ Солдаткина О. А. Возможности применения технологии блокчейн для информатизации судебной системы // Российская юстиция. 2019. № 3. С. 38.

⁵ Солдаткина О. Л. Указ. соч. С. 38—40.

⁶ Масленникова Л. Н., Сушина Т. Е. Оптимизация судебного контроля на начальном этапе уголовного судопроизводства // Российская юстиция. 2019. № 3. С. 41—43 ; Сидоров В. В. Актуальные вопросы применения современных цифровых технологий при реализации принципа обжалования в уголовном судопроизводстве России // Вестник Калининградского юридического института МВД России. 2009. № 2 (18). С. 217—220.

⁷ Бормотова Л. В. Особенности информационно-коммуникационного обеспечения уголовного судопроизводства РФ // Вестник ОГУ. 2013. № 3 (152). С. 24—27 ; Зувев С. В. Цифровая среда уголовного судопроизводства: проблемы и перспективы // Сибирский юридический вестник. 2018. № 4. С. 118—121.

⁸ Абдувалиева А. Ф. Предпосылки и перспективы внедрения электронной формы уголовного дела в деятельность судебных органов // Юридические исследования. 2013. № 5. С. 150—164 ; Познанский Ю. Н. Электронное уголовное дело в решении проблемы расследования уголовных дел в разумные сроки // Труды Академии управления МВД России. 2015. № 1 (33). С. 41—44.

⁹ Марковичева Е. В. Элементы электронного правосудия в российском уголовном процессе // Современное уголовно-процессуальное право России: уроки истории и проблемы дальнейшего реформирования : сб. материалов Междунар. науч.-практ. конф., 20—21 октября 2016 г. Орел, 2016. С. 246—249.

¹⁰ Сидоров Ю. В. Отличия в понимании сущности электронного правосудия в России и за рубежом // Ученые записки Петрозаводского государственного университета. Юридические науки. 2015. Август № 5. С. 108—111.

в новых условиях¹¹, применение электронной подписи в уголовном судопроизводстве и другие вопросы.

Федеральным законом от 23.06.2016 № 220-ФЗ в УПК РФ была введена статья 474.1, регулирующая порядок использования электронных документов в уголовном судопроизводстве применительно к суду. Ходатайство, заявление, жалоба, представление могут быть поданы в суд в форме электронного документа, подписанного лицом, направившим такой документ, электронной подписью в соответствии с законодательством Российской Федерации. Направляется электронный документ в суд посредством заполнения формы, размещенной на официальном сайте суда в информационно-телекоммуникационной сети «Интернет». Судебное решение может быть изготовлено в форме электронного документа, который подписывается судьей усиленной квалифицированной подписью. В случае если судебное решение вынесено судом коллегиально, оно подписывается всеми судьями, участвующими в рассмотрении дела, усиленной квалифицированной подписью. При изготовлении судебного решения в форме электронного документа дополнительно изготавливается экземпляр судебного решения на бумажном носителе.

Поскольку эти нормы регулируют обращение в суд и принятие судебных решений, можно говорить о возможности их применения и к предварительному судебному контролю (рассмотрение жалоб и ходатайств судьей) и о невозможности их применения при обращении с сообщением о преступлении и принятии следователем (дознавателем) решений.

Доступ к правосудию на начальном этапе уголовного судопроизводства в силу публично-правовой природы уголовного судопроизводства по общему правилу обеспечивается государством путем возбуждения и расследования уголовного дела. Серьезным фактором,

препятствующим доступу к правосудию в уголовном судопроизводстве, выступает укрытие от учета преступлений путем отказа в приеме сообщений, отказа в регистрации поступивших сообщений о преступлении. Автоматизированная система регистрации сообщений о преступлении, исключая человеческий фактор, могла бы сыграть существенную роль в обеспечении доступа к правосудию.

Сложная и неповоротливая система досудебного производства создает существенные препятствия для доступа к правосудию в максимально короткие сроки, в том числе по причине принятия незаконных решений, определяющих динамику производства, отсутствия оперативного и действенного контроля за законностью действий (бездействия) и решений, принимаемых в досудебном производстве.

Обстоятельствами, создающими препятствия на пути к правосудию, являются прежде всего незаконные и необоснованные решения, прерывающие (прекращающие, приостанавливающие) досудебное производство на пути к правосудию. К таким решениям следует отнести незаконные отказы в приеме и регистрации сообщений о преступлении, отказы в возбуждении уголовного дела, незаконные и необоснованные решения о приостановлении и прекращении уголовного дела. Одним из серьезных факторов, блокирующих доступ потерпевшего к правосудию, является так называемая предварительная (доследственная) проверка, которая, по сути, выступает суррогатом расследования. Растянутые во времени до бесконечности эти проверки, в том числе и путем незаконных манипуляций с неоднократным вынесением решений об отказе в возбуждении уголовного дела, препятствуют доступу к правосудию.

В современной уголовно-процессуальной теории существуют самые различные понимания и предложения о перестройке досудебного производства, которое позволяло бы обеспе-

¹¹ Пастухов П. С. Электронное вещественное доказательство в уголовном судопроизводстве // Вестник Томского государственного университета. 2015. № 396. С. 149—153 ; Оконенко Р. И. Доказательственное право Российской Федерации и Соединенных Штатов Америки в информационную эпоху: уголовно-процессуальный аспект // Юридический вестник СамГУ. 2015. Т. 1. № 3. С. 145—149 ; Чернышев В. Н., Лоскутова Е. С. Проблемы собирания и использования цифровых доказательств. 2017. Т. 12. № 5. С. 199—203.

чить справедливое судебное разбирательство уголовно-правового спора по существу, не создавая излишней волокиты и позволяя заинтересованным лицам защищать свои законные интересы как на подступах к правосудию, так и в ходе судебного разбирательства. Среди предложений — ликвидация стадии возбуждения уголовного дела¹², введение дознания как этапа, предшествующего следствию¹³, введение судебного следователя или следственного судьи, изменение понимания доказывания и доказательств¹⁴ и многое другое¹⁵.

Не вникая в суть этих предложений, не давая им какой-либо оценки, хотелось бы отметить, что неизменной останется — в силу публично-правовой природы уголовного судопроизводства, уничтожить которую недопустимо, — обязанность государства обеспечить доступ потерпевшего к правосудию. Эта обязанность возложена на государство Конституцией Российской Федерации (ст. 52).

Однако этот начальный этап уголовного судопроизводства может и должен претерпеть существенные изменения. Столь существенные, что можно будет говорить о смене парадигмы досудебного производства, предшествующего правосудию. Лицо, обращающееся к государству с сообщением о преступлении, не должно быть просителем, а должно выступать лицом, инициирующим деятельность государства по установлению всех обстоятельств преступления, о признаках которого сообщается. По сути, государство оказывает услугу, обеспечивая путем

расследования доступ потерпевшего к правосудию. Динамика этого процесса должна быть абсолютно прозрачной и позволять в максимально короткие сроки при наличии к тому оснований обеспечивать доступ к правосудию как потерпевшего от преступления, так и обвиняемого. Кроме того, на начальном этапе уголовного судопроизводства заинтересованные участники должны иметь доступ к судебной власти, инициируя обеспечительные меры для правосудия (например, ходатайство о наложении ареста на имущество, о депонировании доказательств, о производстве действий, направленных на собирание доказательств и пр.). Конституционному положению о состязательности и равноправии сторон в уголовном судопроизводстве противоречит то положение, что на начальном этапе уголовного судопроизводства к судье с ходатайством за обеспечительными мерами могут обратиться только представители государства (следователь, дознаватель), а не любой заинтересованный в правосудии участник уголовного судопроизводства.

Ключевым моментом в трансформации досудебного производства должно стать электронное взаимодействие государства и общества (населения) в новой цифровой реальности. Появляются принципиально новые возможности участия в уголовном судопроизводстве (в том числе в удаленном доступе) и новые возможности влияния на принятие решений и контроль за принятием решений (автоматизация регистрации сообщения о преступлении и начала

¹² *Гаврилов Б. Я.* Роль института возбуждения уголовного дела в обеспечении прав потерпевших на их доступ правосудию // Вестник Сибирского юридического института МВД России. 2018. № 2 (31). С. 19—27.

¹³ *Гирько С. И.* Производство по уголовному делу дознания в сокращенной форме: прогнозы и суждения // Российский следователь. 2013. № 21. С. 2—5.

¹⁴ *Александров А. С.* О доктринальной модели современного доказательственного права России // Вестник Нижегородской правовой академии. 2015. № 5. С. 7—11.

¹⁵ *Акперов Р. С.* Возбуждение уголовного дела в уголовно-процессуальном праве Российской Федерации : автореф. дис. ... канд. юрид. наук. Самара, 2010 ; *Рябополова Я. П.* Процессуальные действия, проводимые в стадии возбуждения уголовного дела: правовые, теоретические и организационные основы : автореф. дис. ... канд. юрид. наук. М., 2013 ; *Кожокаръ В. В.* Возбуждение уголовного дела: вопросы теории и практики : автореф. дис. ... канд. юрид. наук. М., 2016 ; *Борозонец Н. Н.* Правообеспечительная деятельность прокурора в стадии возбуждения уголовного дела : автореф. дис. ... канд. юрид. наук. Краснодар, 2016 ; *Таболкина К. А.* Надзор прокурора за возбуждением и расследованием уголовных дел : автореф. дис. ... канд. юрид. наук. М., 2016.

расследования, возможность подачи жалоб, ходатайств, получение копий решений в электронном виде).

Мировая картинка «Индустрия 4.0» завораживает, и это действительно близкое будущее. Все чаще слышим мы о цифровой трансформации (трансформации права, трансформации уголовного судопроизводства). Понятно, что трансформация как изменение — это процесс. Процесс достаточно длительный.

Надо полагать, что цифровая трансформация досудебного производства — это длительный процесс, а не быстрый результат. Словосочетание «цифровая трансформация» сразу вводит в заблуждение. Однако главное слово — «трансформация». Досудебное производство должно стать гибкой организационной структурой с возможностью молниеносного принятия решений, с невероятно высоким уровнем взаимодействия, высокой мотивацией к инновациям и такой же толерантностью к риску. Однако необходим принципиально новый алгоритм (законодательная модель) начального этапа уголовного судопроизводства, обеспечивающего доступ к правосудию. Необходимо исключить на начальном этапе уголовного судопроизводства все лишнее, затратное, не имеющее процессуального смысла, лишнее процессуальных гарантий (доследственная проверка, сокращенное дознание и др.).

Взаимодействие государства с населением подразумевает сильные горизонтальные связи (платформа электронного взаимодействия государственных органов и заинтересованных лиц). Взаимодействие государственных структур должно подразумевать строгую вертикальную иерархию (платформа электронного взаимодействия между государственными органами по вертикали, например в прокуратуре или МВД). Будущее досудебного производства, которое должно обеспечивать в уголовном судопроизводстве доступ к правосудию, за горизонтальным сотрудничеством, участником которого являются государство и граждане.

Становится очевидным, что высокая зрелость ИТ в организации уголовного судопроизводства становится необходимым, но недостаточным условием для трансформации досудебного произ-

водства в гибкую организацию, так как вопросы культуры, структуры досудебного производства, порядков принятия решений являются первоочередными для совершения технологического прорыва в уголовном судопроизводстве, в частности в досудебном производстве.

Цифровая трансформация досудебного производства — это не про цифровизацию, а об изменении сути обеспечения доступа к правосудию на начальном этапе уголовного судопроизводства с высокой зрелостью ИТ, в том числе и судебной властью. При этом судебная власть на начальном этапе уголовного судопроизводства должна приобрести принципиально иное значение, стать независимым самостоятельным судебным органом с отлаженной службой судебных приставов, исполняющих судебные решения по результатам рассмотрения ходатайств. Цифровая трансформация досудебного производства в первую очередь затрагивает организационную трансформацию, изменение начального этапа уголовного судопроизводства (так называемого досудебного производства и всех сопутствующих производств) и только во вторую очередь приносит «цифру» в уголовное судопроизводство, в частности на начальный этап уголовного судопроизводства, обеспечивающий доступ к правосудию в уголовном судопроизводстве.

Цифровая трансформация уголовного судопроизводства в части обеспечения доступа к правосудию невозможна, если не осознать необходимость новой парадигмы начального этапа уголовного судопроизводства, обеспечивающего доступ к правосудию.

Сегодня мы пытаемся, как это следует из публикаций, вместить новую реальность, именуемую Industry 4.0, в прокрустово ложе действующей парадигмы уголовного судопроизводства, в частности досудебного производства, хотя признаем его хаотичность, неэффективность, по сути обслуживание ведомственных интересов, а не защиту законных интересов и конституционных прав граждан России.

Действующая парадигма уголовного судопроизводства (начальный этап, предшествующий правосудию) заключается в господстве следующих идей и практик:

- уголовное судопроизводство построено по стадиям;
- в структуре уголовного судопроизводства выделяют досудебное производство, представленное 2 стадиями — возбуждение и расследование уголовного дела;
- расследование представлено 3 формами — предварительное следствие, дознание, сокращенное дознание;
- досудебное производство формально находится под контролем судьи, надзором прокурора, контролем начальника органа расследования;
- следователь (дознатель) фактически лишен самостоятельности, пассивен и озадачен лишь формальной оценкой его деятельности по критериям, установленным ведомством;
- уголовное дело — это фиксация в письменной форме всех действий и решений государственных органов и должностных лиц (действия — протоколами, решения постановлениями, запросы и ответы) и частных лиц в виде обращений с жалобами и ходатайствами;
- уголовное дело, сформированное в досудебном производстве, как правило, основа для принятия решений судом.

Новая парадигма уголовного судопроизводства, обеспечивающего доступ к правосудию, — это, по сути, модель постановки проблемы обеспечения доступа к правосудию в уголовном судопроизводстве и ее решения, это концептуальная схема обеспечения доступа к правосудию в уголовном судопроизводстве в современном мире применительно к уровню развития России в новой цифровой реальности.

Новая парадигма рождается из аномалии, к которой мы не привыкли. Суть ее в том, что государство оказывает услугу по обеспечению доступа к правосудию в уголовном судопроизводстве, в том числе и путем формирования и обоснования уголовно-правовой претензии о нарушении уголовно-правового запрета. Понимание деятельности государства как услуги, которую оно оказывает населению, — это и есть аномалия нашего мировоззрения. Но именно из нее и может родиться новая парадигма уголовного судопроизводства, обеспечивающего

доступ к правосудию. Именно эта аномалия может, по сути, все поставить на свои места. Главное в уголовном судопроизводстве — это рассмотрение уголовно-правового спора по существу в суде первой инстанции (правосудие). Однако специфика уголовного судопроизводства в том, что необходимо обеспечить доступ к правосудию, и обязанность эта возложена на государство. Однако данное обстоятельство не должно лишать население России возможностей влиять на подготовку к правосудию, в том числе и путем обращения к судебной власти, подавая ходатайства и жалобы, в том числе в электронном виде.

Решение отказаться от старой парадигмы всегда одновременно решение принять новую парадигму. Смене парадигмы, как правило, предшествует кризис, переживаемый старой парадигмой. Это существенно облегчает революционный момент смены парадигмы. Следует признать в современной России банкротство существующих правил досудебного производства, которое означает поиск новых.

Изменение парадигмы связано с изменением ключевых понятий. «Досудебное производство» следует рассматривать как начальный этап уголовного судопроизводства, направленный на обеспечение доступа к правосудию. На этом начальном этапе (с момента регистрации сообщения о преступлении до поступления дела в суд для рассмотрения уголовно-правового спора о виновности) в единую электронную систему обеспечения доступа к правосудию должны быть соединены государственные органы (суд, прокурор, следователь, дознаватель) и лица, заинтересованные в достижении правосудия.

Расследование должно начинаться незамедлительно и должно быть направлено на установление наличия преступления и лица, его совершившего, с целью обеспечения доступа к правосудию. Прокурор обеспечивает доступ к правосудию путем надзора за формированием обвинения и его утверждения, за законностью принятия процессуальных решений. На начальном этапе уголовного судопроизводства, обеспечивающего доступ к правосудию, принципиально должно измениться значение судебной власти. Необходим независимый и са-

мостоятельный судебный орган, обеспечивающий доступ к правосудию путем рассмотрения жалоб и ходатайств. Заявить ходатайство к суду об обеспечительных мерах должны иметь право не только представители государства, но и иные заинтересованные участники.

Единая система обеспечения доступа к правосудию должна быть разработана как законодательная модель, представляющая собой алгоритм для цифровой трансформации в единую платформу электронного взаимодействия государства и населения, обеспечивающую доступ к правосудию в уголовном судопроизводстве.

Цифровая трансформация досудебного производства может быть достигнута главным образом за счет рационального управления системами автоматизации регистрации сообщения о преступлении, расследования, принятия решений, обеспечивающих доступ к правосудию, проверки их законности и обеспечительных мер судебного органа, обеспечивающего доступ к правосудию, интегрированных в единое информационное пространство.

Необходима разработка стратегии цифровой трансформации досудебного производства

в начальный этап уголовного судопроизводства, обеспечивающий доступ к правосудию, включающая разработку и внедрение технологических решений (сквозная интеграция IT-продукта, автоматизация сбора данных, внедрение алгоритмов искусственного интеллекта и др.), исключая цифровое неравенство.

Концепция построения уголовного судопроизводства, обеспечивающего доступ к правосудию, в новой цифровой реальности может стать парадигмой в силу своей привлекательности в данную эпоху. Привлекательность этой идеи заключается не в последнюю очередь в надежде на ее продуктивность, ибо эта идея будет работать в интересах населения России. Хотя, безусловно, найдутся и те, кто будет говорить о компанейщине применительно к развитию уголовного судопроизводства в свете цифровых технологий. Активно отрицать любые изменения, тем более связанные с цифровой трансформацией, будут представители государства, которые консервативны в принципе и ничего не хотят менять, полагая, что любые изменения должны быть выгодны им, а не населению страны.

БИБЛИОГРАФИЯ

1. Абдувалиева А. Ф. Предпосылки и перспективы внедрения электронной формы уголовного дела в деятельность судебных органов // Юридические исследования. — 2013. — № 5. — С. 150—164.
2. Акперов Р. С. Возбуждение уголовного дела в уголовно-процессуальном праве Российской Федерации : автореф. дис. ... канд. юрид. наук. — Самара, 2010.
3. Александров А. С. О доктринальной модели современного доказательственного права России // Вестник Нижегородской правовой академии. — 2015. — № 5. — С. 7—11.
4. Бормотова Л. В. Особенности информационно-коммуникационного обеспечения уголовного судопроизводства РФ // Вестник ОГУ. — 2013. — № 3 (152). — С. 24—27.
5. Борозонец Н. Н. Правообеспечительная деятельность прокурора в стадии возбуждения уголовного дела : автореф. дис. ... канд. юрид. наук. — Краснодар, 2016.
6. Быков А. Ю. Право цифровой экономики: некоторые народно-хозяйственные и политические риски. — М. : Проспект, 2018.
7. Гаврилов Б. Я. Роль института возбуждения уголовного дела в обеспечении прав потерпевших на их доступ правосудию // Вестник Сибирского юридического института МВД России. — 2018. — № 2 (31). — С. 19—27.
8. Гирько С. И. Производство по уголовному делу дознания в сокращенной форме: прогнозы и суждения // Российский следователь. — 2013. — № 21. — С. 2—5.
9. Зуев С. В. Цифровая среда уголовного судопроизводства: проблемы и перспективы // Сибирский юридический вестник. — 2018. — № 4. — С. 118—121.

10. *Кожокарь В. В.* Возбуждение уголовного дела: вопросы теории и практики : автореф. дис. ... канд. юрид. наук. — М., 2016.
11. *Марковичева Е. В.* Элементы электронного правосудия в российском уголовном процессе // Современное уголовно-процессуальное право России: уроки истории и проблемы дальнейшего реформирования : сб. материалов Междунар. науч.-практ. конф., 20—21 октября 2016 г. — Орел, 2016. — С. 246—249.
12. *Масленникова Л. Н., Сушина Т. Е.* Оптимизация судебного контроля на начальном этапе уголовного судопроизводства // Российская юстиция. — 2019. — № 3. — С. 41—43.
13. *Оконенко Р. И.* Доказательственное право Российской Федерации и Соединенных Штатов Америки в информационную эпоху: уголовно-процессуальный аспект // Юридический вестник СамГУ. — 2015. — Т. 1. — № 3. — С. 145—149.
14. Основы цифровой экономики : учебное пособие / колл. авт. ; под ред. М. И. Столбова, Е. А. Бренделевой. — М. : Научная библиотека, 2018.
15. *Пастухов П. С.* Электронное вещественное доказательство в уголовном судопроизводстве // Вестник Томского государственного университета. — 2015. — № 396. — С. 149—153.
16. *Познанский Ю. Н.* Электронное уголовное дело в решении проблемы расследования уголовных дел в разумные сроки // Труды Академии управления МВД России. — 2015. — № 1 (33). — С. 41—44.
17. *Рябополова Я. П.* Процессуальные действия, проводимые в стадии возбуждения уголовного дела: правовые, теоретические и организационные основы : автореф. дис. ... канд. юрид. наук. — М., 2013.
18. *Сидоров В. В.* Актуальные вопросы применения современных цифровых технологий при реализации принципа обжалования в уголовном судопроизводстве России // Вестник Калининградского юридического института МВД России. — 2009. — № 2 (18). — С. 217—220.
19. *Сидоров Ю. В.* Отличия в понимании сущности электронного правосудия в России и за рубежом // Ученые записки Петрозаводского государственного университета. Юридические науки. — 2015. — Август № 5. — С. 108—111.
20. *Солдаткина О. Л.* Возможности применения технологии блокчейн для информатизации судебной системы // Российская юстиция. — 2019. — № 3. — С. 38—40.
21. *Таболкина К. А.* Надзор прокурора за возбуждением и расследованием уголовных дел : автореф. дис. ... канд. юрид. наук. — М., 2016.
22. *Чернышев В. Н., Лоскутова Е. С.* Проблемы собирания и использования цифровых доказательств. — 2017. — Т. 12. — № 5. — С. 199—203.
23. *Шваб К.* Четвертая промышленная революция. — М. : Э, 2017.

Материал поступил в редакцию 6 мая 2019 г.

TRANSFORMATION OF PRE-TRIAL PROCEEDINGS IN THE INITIAL STAGE OF CRIMINAL PROCEEDINGS, ENSURING ACCESS TO JUSTICE IN THE INDUSTRY 4.0 ERA¹⁶

MASLENNIKOVA Larissa Nikolaevna, Doctor of Law, Professor, Professor of the Department of Criminal Procedure Law of the Kutafin Moscow State Law University (MSAL)
mln1954@yandex.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

Abstract. *The paper deals with topical issues of ensuring access to justice in criminal proceedings, and substantiates the need to change the paradigm of the pre-trial proceedings. The new digital reality Industry 4.0 assumes a tremendous pace of development, profound changes in all spheres of society, including criminal proceedings. The author argues that the digital transformation of criminal proceedings in terms of ensuring access to justice is impossible unless the legislative model (algorithm) of the initial stage of criminal proceedings ensuring access to justice is changed. The key point in the transformation of the pre-trial proceedings should be the electronic interaction of the state and society (population) in the new digital reality. There are fundamentally new opportunities for participation in criminal proceedings (including remotely) and new opportunities to influence decision making and control over decision making (automatization of a crime report and the start of investigation registration, the ability to file complaints, petitions, receive notifications, copies of decisions in electronic form).*

Keywords: *criminal proceedings, initial stage, access to justice, pre-trial proceedings, digital transformation, paradigm shift, state service, crime report registration automation, electronic interaction, electronic document.*

REFERENCES (TRANSLITERATION)

1. Abduvalieva A. F. Predposylki i perspektivy vnedreniya elektronnoy formy ugovolnogo dela v deyatelnost' sudebnyh organov // Yuridicheskie issledovaniya. — 2013. — № 5. — S. 150—164.
2. Akperov R. S. Vozbuzhdenie ugovolnogo dela v ugovolno-processual'nom prave Rossijskoj Federacii : avtoref. dis. ... kand. jurid. nauk. — Samara, 2010.
3. Aleksandrov A. S. O doktrinal'noj modeli sovremennogo dokazatel'stvennogo prava Rossii // Vestnik Nizhegorodskoj pravovoj akademii. — 2015. — № 5. — S. 7—11.
4. Bormotova L. V. Osobennosti informacionno-kommunikacionnogo obespecheniya ugovolnogo sudoproizvodstva RF // Vestnik OGU. — 2013. — № 3 (152). — S. 24—27.
5. Borozonec N. N. Pravoobespechitel'naya deyatelnost' prokurora v stadii vozbuzhdeniya ugovolnogo dela : avtoref. dis. ... kand. jurid. nauk. — Krasnodar, 2016.
6. Bykov A. Yu. Pravo cifrovoj ekonomiki: nekotorye narodno-hozyajstvennye i politicheskie riski. — M. : Prospekt, 2018.
7. Gavrilov B. Ya. Rol' instituta vozbuzhdeniya ugovolnogo dela v obespechenii prav poterpevshih na ih dostup pravosudiyu // Vestnik Sibirskogo yuridicheskogo instituta MVD Rossii. — 2018. — № 2 (31). — S. 19—27.
8. Gir'ko S. I. Proizvodstvo po ugovolnomu delu doznaniya v sokrashchennoj forme: prognozy i suzheniya // Rossijskij sledovatel'. — 2013. — № 21. — S. 2—5.
9. Zuev S. V. Cifrovaya sreda ugovolnogo sudoproizvodstva: problemy i perspektivy // Sibirskij yuridicheskij vestnik. — 2018. — № 4. — S. 118—121.

¹⁶ The publication is prepared with the financial support of the Russian Foundation for Basic Research, Research Project No. 18-29-16018 «The concept of building criminal proceedings providing access to justice in the conditions of the development of digital technologies».

10. Kozhokar' V. V. Vozbuzhdenie ugovnogo dela: voprosy teorii i praktiki : avtoref. dis. ... kand. jurid. nauk. — M., 2016.
11. Markovicheva E. V. Elementy elektronnoho pravosudiya v rossijskom ugovnom processe // Sovremennoe ugovno-processual'noe pravo Rossii: uroki istorii i problemy dal'nejshego reformirovaniya : sb. materialov Mezhdunar. nauch.-prakt. konf., 20—21 oktyabrya 2016 g. — Orel, 2016. — S. 246—249.
12. Maslennikova L. N., Sushina T. E. Optimizaciya sudebnogo kontrolya na nachal'nom etape ugovnogo sudoproizvodstva // Rossijskaya yusticiya. — 2019. — № 3. — S. 41—43.
13. Okonenko R. I. Dokazatel'stvennoe pravo Rossijskoj Federacii i Soedinennyh Shtatov Ameriki v informacionnuju epohu: ugovno-processual'nyj aspekt // Yuridicheskij vestnik SamGU. — 2015. — T. 1. — № 3. — S. 145—149.
14. Osnovy cifrovoj ekonomiki : uchebnoe posobie / koll. avt. ; pod red. M. I. Stolbova, E. A. Brendelevoj. — M. : Nauchnaya biblioteka, 2018.
15. Pastuhov P. S. Elektronnoe veshchestvennoe dokazatel'stvo v ugovnom sudoproizvodstve // Vestnik Tomskogo gosudarstvennogo universiteta. — 2015. — № 396. — S. 149—153.
16. Poznanskij Yu. N. Elektronnoe ugovnoe delo v reshenii problemy rassledovaniya ugovnyh del v razumnye sroki // Trudy Akademii upravleniya MVD Rossii. — 2015. — № 1 (33). — S. 41—44.
17. Ryabopolova Ya. P. Processual'nye dejstviya, provodimye v stadii vozbuzhdeniya ugovnogo dela: pravovye, teoreticheskie i organizacionnye osnovy : avtoref. dis. ... kand. jurid. nauk. — M., 2013.
18. Sidorov V. V. Aktual'nye voprosy primeneniya sovremennyh cifrovych tekhnologij pri realizacii principa obzhalovaniya v ugovnom sudoproizvodstve Rossii // Vestnik Kaliningradskogo yuridicheskogo instituta MVD Rossii. — 2009. — № 2 (18). — S. 217—220.
19. Sidorov Yu. V. Otlichiya v ponimanii sushchnosti elektronnoho pravosudiya v Rossii i za rubezhom // Uchenye zapiski Petrozavodskogo gosudarstvennogo universiteta. Yuridicheskie nauki. — 2015. — Avgust № 5. — S. 108—111.
20. Soldatkina O. L. Vozmozhnosti primeneniya tekhnologii blokchejn dlya informatizacii sudebnoj sistemy // Rossijskaya yusticiya. — 2019. — № 3. — S. 38—40.
21. Tabolina K. A. Nadzor prokurora za vozbuzhdeniem i rassledovaniem ugovnyh del : avtoref. dis. ... kand. jurid. nauk. — M., 2016.
22. Chernyshev V. N., Loskutova E. S. Problemy sobiraniya i ispol'zovaniya cifrovych dokazatel'stv. — 2017. — T. 12. — № 5. — S. 199—203.
23. Shvab K. Chetvertaya promyshlennaya revolyuciya. — M. : E, 2017.

К. В. Обидин*

О соотношении основания для возбуждения уголовного дела и оснований для предъявления обвинения в условиях цифровизации уголовного судопроизводства¹

Аннотация. Распространение и активное использование технических средств аудио- и видеофиксации в процессе выявления и доказывания отдельных видов преступлений приводит к необходимости переосмысления соотношения некоторых теоретических понятий. В статье анализируются схожие элементы и различия основания для возбуждения уголовного дела и оснований для предъявления обвинения. Обращается внимание на сближение содержания данных понятий в условиях распространения цифровых технологий в уголовном судопроизводстве. Высказывается мнение о том, что использование аудио- и видеозаписей в процедуре познания оказывает существенное влияние на внутреннее убеждение следователя и дознавателя при принятии процессуальных решений. Анализируется возможность возбуждения уголовного дела исключительно на основании аудио- и видеозаписи. Излагается точка зрения о недопустимости упрощения процедуры доказывания в случаях наличия аудио- и видеозаписей вместе с признательными показаниями, поскольку в таком случае имеет место нарушение базовых основ познавательной деятельности в рамках уголовного судопроизводства.

Ключевые слова: цифровизация, аудио- и видеозаписи, основание для возбуждения уголовного, основания для предъявления обвинения, доказывание, достаточность, взяточничество.

DOI: 10.17803/1994-1471.2019.103.6.147-155

Активное использование цифровых технологий в судопроизводстве является одним из приоритетных направлений развития современного российского общества. Государство выделяет значительные денежные средства на создание, развитие и содержание информационно-правовых баз, техническое оснащение судов современными средствами аудио- и видеофиксации, а также создание цифрового пространства, упрощающего взаимодействие с государственными органами. Наличие

положительных изменений, демонстрирующих работу над оптимизацией и повышением качества процессуальной деятельности, не отменяет, однако, того факта, что отдельные отрасли права проявляют «малую мобильность», а их представители традиционно придерживаются наиболее консервативных взглядов как в науке, так и на практике. Ярким примером подобного подхода является современная система уголовного судопроизводства России, крайне аккуратно изменяющаяся в направлении цифровизации системы

¹ Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16041.МК.

© Обидин К. В., 2019

* Обидин Кирилл Вячеславович, международное адвокатское бюро «Глинка, Рубинштейн и партнеры», стажер

obidinkirill.2018@gmail.com

107045, Россия, г. Москва, Сретенский бульв., д. 5

государственного управления, определенного руководством страны².

С одной стороны, необходимость дополнительной проверки любых потенциальных изменений в рассматриваемой сфере объясняется спецификой регулируемых общественных отношений, связанных с защитой и восстановлением приоритетных прав и свобод человека. С другой — современное уголовно-процессуальное законодательство является прямым наследником УПК РСФСР, разработанного с учетом темпов развития общественных отношений 60-х гг. прошлого столетия, несопоставимых с прогрессом человечества в XXI в.

Одним из последствий стремительной «революции» человеческой мысли стала цифровизация, коснувшаяся в том числе и уголовного судопроизводства. Это явление не ограничивается только внедрением отдельных технологических достижений в уже сформировавшиеся механизмы юридической деятельности, но приводит к необходимости формирования качественно новых требований к способам регулирования общественных отношений в иных, «цифровых» условиях существования общества и государства.

Ярким примером подобных изменений является повсеместное внедрение и распространение средств аудио- и видеофиксации, которые, помимо прочего, являются не только способом детального закрепления фактов и обстоятельств, но и эффективным инструментом доказывания (более 70 % всех правонарушений в г. Москве расследуется с использованием городской системы видеонаблюдения; в 2017 г. число преступлений, раскрытых с ее использованием, составило 3 085 дел)³.

Особый интерес вызывает вопрос готовности современной уголовно-процессуальной теории к вызовам достижений науки, поскольку некоторые устоявшиеся правовые конструкции и механизмы требуют совершенствования с учетом технических возможностей, предоставляемых в настоящее время. В рамках данной статьи речь пойдет о влиянии цифровизации на соотношение таких базовых понятий, как «основание для возбуждения уголовного дела» и «основания для предъявления обвинения».

Предусмотренная ч. 2 ст. 140 УПК РФ конструкция основания для возбуждения уголовного дела выстроена вокруг крайне неоднозначного термина «достаточные данные». В научной литературе неоднократно указывалось на оценочный характер конструкции, свидетельствующий о необходимости индивидуального подхода к каждому случаю проверки сообщения о преступлении⁴. Объемы проводимых проверочных мероприятий исходя из буквального толкования закона ограничены исключительно временем, предоставляя уполномоченному органу возможность формировать собственное субъективное мнение о допустимости принятия итогового для стадии процессуального решения. Несмотря на это, следует поддержать позицию ученых, высказывающихся о необходимости ограничения достаточности данных задачами стадии возбуждения уголовного дела⁵. Цель проведения проверочных мероприятий заключается не в сборе доказательств преступления, а в получении сведений, свидетельствующих пока только о совершении деяния, содержащего отдельные признаки преступного деяния. Именно поэтому в уголовно-процессуальной науке

² Послание Президента РФ В. В. Путина Федеральному Собранию от 1 марта 2018 г. // Официальный сайт Президента РФ. URL: <http://www.kremlin.ru/events/president/news/56957>.

³ Презентация к отчету «О выполнении Государственной программы города Москвы «Безопасный город» в 2017 году и задачах по обеспечению безопасности города Москвы на 2018 год» // Официальный сайт Мера Москвы. URL: <https://www.mos.ru/drbez/documents/programma-bezopasnyi-gorod/view/215646220/>.

⁴ Уголовно-процессуальное право Российской Федерации : учебник / отв. ред. П. А. Лупинская, Л. А. Воскобитова. 4-е изд., перераб. и доп. М. : Норма: Инфра-М, 2018. С. 432 ; Уголовно-процессуальное право Российской Федерации : учебник для вузов / под общ. ред. Г. М. Резника. М. : Юрайт, 2013. С. 425.

⁵ Уголовно-процессуальное право (Уголовный процесс) : учебник для студентов вузов, обучающихся по направлению подготовки «Юриспруденция» / под ред. А. В. Ендольцевой, О. В. Химичевой, Е. Н. Клециной. М. : Юнити-Дана: Закон и право, 2015. С. 298.

стадия возбуждения уголовного дела неразрывно ассоциируется с вероятностными выводами, т.е. обоснованными предположениями⁶. Среди процессуалистов встречается мнение о том, что минимальным порогом принятия решения является подтверждение наличия события (деяния), соотносимого с объективной стороной и объектом преступления⁷. В результате проводимая подобным образом проверочная процедура направлена на отграничение уголовно наказуемого деяния от действий, порождающих административные, гражданско-правовые или иные отношения⁸.

Напротив, при рассмотрении понятия «основания для предъявления обвинения» речь идет о закономерном итоге проведенной ранее познавательной деятельности, позволившей уполномоченному лицу собрать «достаточные доказательства» совершения инкриминируемого преступления.

Аналогично со стадией возбуждения уголовного дела достаточность является оценочной категорией. Специалисты в области уголовного процесса обоснованно указывают на комплексную трехэлементную структуру оснований для предъявления обвинения, определяющую совокупность факторов, в отсутствии которых осуществление столь значимой процессуальной деятельности недопустимо (фактическое, процессуальное и юридическое основание)⁹. В результате необходимо не только достоверно установить обстоятельства, предусмотренные ст. 73 УПК РФ, но также собрать такой объем доказательств, отвечающих критериям относимости, допустимости и достоверности, который

позволит стороне обвинения утверждать о наличии в деянии лица всех признаков состава преступления. На данной стадии досудебного производства непозволительно выстраивание публично-правовой претензии государства на основе предположения¹⁰.

Таким образом, сочетание конструкции основания для возбуждения уголовного дела, базирующейся на достаточных данных, и системы оснований для предъявления обвинения, выстроенной из достаточных доказательств, показывает последовательность познавательной деятельности уполномоченного должного лица. Имеет место наглядный переход от предположения к убежденности в наличии преступления, а также установленности совершившего его лица.

В результате критерием дифференциации рассматриваемых теоретических понятий является не что иное, как субъективное мнение следователя и дознавателя, подкрепленное собранными, проверенными и оцененными сведениями. В условиях расширения внедрения цифровых технологий в уголовное судопроизводство, в частности активного использования аудио- и видеозаписей, этот вывод порождает ряд вопросов, имеющих принципиальное значение как для теории, так и для практики.

Аудио- и видеозаписи представляют собой особый источник сведений, требующий дополнительного теоретического осмысления. При этом совершенно очевидно, что технические возможности, существующие в настоящее время в распоряжении не только государства, но и частных лиц, выводят этот источник сведе-

⁶ Курс уголовного процесса / под ред. д. ю. н., профессора Л. В. Головки. 2-е изд., испр. М. : Статут, 2017. С. 606.

⁷ Уголовный процесс : учебник / А. В. Смирнов, К. Б. Калиновский ; под общ. ред. проф. А. В. Смирнова. 4-е изд., перераб. и доп. М. : Кнорус, 2008. С. 327.

⁸ Уголовный процесс : учебник для бакалавриата юридических вузов / О. И. Андреева [и др.] ; под ред. О. И. Андреевой, А. Д. Назарова, Н. Г. Стойко и А. Г. Тузова. Ростов н/Д : Феникс, 2015. С. 183.

⁹ Уголовно-процессуальный кодекс Российской Федерации. Главы 1—32.1 : постатейный науч.-практ. комментарий / Е. К. Антонович, Е. А. Артамонова, Д. П. Великий [и др.] ; отв. ред. Л. А. Воскобитова. М. : Редакция «Российской газеты», 2015. Вып. III—IV. С. 349.

¹⁰ *Россинский С. Б.* Правовые условия применения мер уголовно-процессуального пресечения приводят к поспешности и необоснованности обвинения // *Законы России: опыт, анализ, практика.* 2018. № 5. С. 30—36.

ний на беспрецедентный по информативности и потенциалу познания уровень. При сравнении наиболее распространенного вида доказательств — свидетельских показаний¹¹ — с аудио- и видеозаписями становится очевидно, что в ряде случаев последние обладают существенными преимуществами. В первую очередь свидетельские показания традиционно относятся к личным доказательствам, т.е. носителем данной информации является человек, воспринимающий, запоминаящий, а впоследствии воспроизводящий полученные сведения¹². Аудио- и видеозаписи, напротив, представляют собой вещественные (материальные) доказательства, позволяющие субъекту доказывания выступить в роли «непосредственного наблюдателя (слушателя)». Применительно к рассматриваемому вопросу имеет место не отдельный вид доказательств, а определенная классификационная группа¹³.

Во-вторых, свидетельские показания существенно зависят от временных рамок. В силу объективных физиологических особенностей с течением времени память человека об обстоятельствах и о фактах (за редкими исключениями) ухудшается. В результате зачастую в случаях несоответствия показаний, данных на досудебной и судебной стадиях, используется механизм оглашения показаний, предусмотренный ч. 3 ст. 281 УПК РФ. При этом правоприменитель

весьма лояльно относится к аргументации невозможности детального восстановления обстоятельств в связи с давностью событий¹⁴. В-третьих, в отличие от свидетельских показаний, аудио- и видеозаписи не нуждаются в проверке на заинтересованность. Несмотря на то что законодатель относит свидетеля к иным участникам уголовного судопроизводства, выделяемым в особую группу в связи с «процессуальной нейтральностью», в теории высказываются соображения о необходимости введения подобного критерия в качестве характеристики участников уголовного судопроизводства¹⁵.

Безусловно, аудио- и видеозаписи не лишены недостатков. Как отмечалось ранее, они могут стать объектом фальсификации¹⁶. Однако в этом случае, в отличие от показаний свидетелей, возможно привлечение лиц, обладающих специальными знаниями, позволяющими выявить воздействие на источник информации. Главный недостаток аудио- и видеозаписей заключается в их фрагментарности, возможности «вырвать из контекста» отдельные действия лица или события. Поэтому актуализируется значение способностей сотрудников правоохранительных органов корректно интерпретировать полученные таким путем сведения и давать им правовую оценку.

Все вышесказанное приводит к вопросу о последствиях применения цифровых технологий

¹¹ Рыжаков А. П. Показания свидетеля — самый распространенный вид доказательств. Комментарий к статье 79 УПК РФ // СПС «КонсультантПлюс», 2006 ; Основы уголовного судопроизводства : учебник для бакалавров / М. В. Бубчикова, В. А. Давыдов, В. В. Ершов [и др.] ; под ред. В. А. Давыдова, В. В. Ершова. М. : РГУП, 2017. С. 119—127.

¹² Теория доказательств в советском уголовном процессе / отв. ред. Н. В. Жогин. Изд. 2-е испр. и доп. М. : Юрид. лит., 1973. С. 257—263 ; Левченко О. В. Классификация доказательств в уголовном процессе // Вестник Оренбургского государственного университета. 2013. № 3 (152). С. 111—114.

¹³ О необходимости разграничения нескольких значений понятия «вещественное доказательство» см.: Курс уголовного процесса / под ред. д. ю. н., проф. Л. В. Головки. 2-е изд., испр. М. : Статут, 2017. С. 459—460.

¹⁴ Апелляционное определение Приморского краевого суда от 14.10.2015 по делу № 22-6269/15 // СПС «КонсультантПлюс» ; приговор Свердловского областного суда от 10.04.2017 по делу № 1-1/2017 // СПС «КонсультантПлюс» ; приговор Московского городского суда от 21.04.2017 № 2-23/2017 // СПС «КонсультантПлюс».

¹⁵ Гарусов А. В. О некоторых проблемах оценки показаний лиц, заинтересованных в исходе уголовного дела // Вестник Санкт-Петербургского университета МВД России. 2016. № 2 (70). С. 60—64.

¹⁶ Завидов Б. Д., Кузнецов Н. П. Проблемы доказательств и доказывания в уголовном судопроизводстве // СПС «КонсультантПлюс», 2004.

в уголовном судопроизводстве. Качество и распространённость средств аудио- и видеозаписи уже в настоящее время позволяют предоставить детальные сведения о событии, подлежащем оценке на наличие в действиях запечатленных лиц признаков состава преступления. В подобных условиях возникает тенденция к фактическому сближению содержания рассматриваемых «оснований», поскольку убежденность следователя (дознателя) может напрямую зависеть от объема информации, содержащегося на аудио- и видеозаписях. Таким образом, на этапе инициирования уголовно-процессуальной деятельности проверяющий орган уже получает в распоряжение сведения, не только являющиеся «достаточными данными» для возбуждения уголовного дела, но и во многом определяющие направление и основу познавательной деятельности.

На практике подобная ситуация существенно изменила процедуру доказывания отдельных видов преступлений, в частности взяточничества. Латентность подобной преступной активности в сочетании с проблемами выявления возможности провокационного поведения привели к тому, что в подавляющем большинстве уголовных дел (95 %) аудио- и видеозапись используется в качестве необходимого источника сведений, на основе которого возбуждается уголовное дело и выстраивается вся процедура доказывания¹⁷. Подобная ситуация наблюдается и при доказывании других видов преступлений, совершаемых в общественных местах: на стадионах, в торговых центрах, на транспорте.

Учитывая все вышесказанное, нерешенными остаются следующие вопросы:

1. В условиях очевидности для поверяющего лица возможно ли возбуждение уголовного дела исключительно на основании аудио- и видеозаписи?

Проблема формулирования однозначного вывода на данный вопрос заключается в необходимости поиска баланса между ограничением прав лиц, причастных к обстоятельствам, повлекшим возбуждение уголовного дела; защитой потенциально нарушенных прав граждан, общества, государства и надлежащим исполнением обязанностей сотрудниками правоохранительных органов. Как справедливо отмечал А. Ф. Кони, возбуждение уголовного преследования «должно слагаться из двоякого рода действий: из проверки сведений, дающих основание и даже обязывающих начать уголовное преследование, и из самого начатия преследования путем предложений о производстве следствия, привлечения обвиняемого и принятии против него предупредительных от побега мер. Уголовное преследование слишком серьезная вещь, чтобы не вызывать самой тщательной обдуманности»¹⁸. Помимо внутренних «фильтров» принятия процессуальных решений, имеют место внешние, выражающиеся в полномочиях суда, руководителя следственного органа и прокурора проверять законность и обоснованность действий сотрудника. В результате неизбежна дополнительная осторожность следователя и дознателя в процессе собирания, проверки и оценки материалов проверки сообщения о преступлении.

С другой стороны, высокая степень критерия оценочности при принятии обоснованного решения о возбуждении уголовного дела должна свидетельствовать о свободе усмотрения должностного лица. Стоит отметить, что достаточность в уголовном судопроизводстве представляет собой совокупность количественного и качественного показателей, сочетание которых должно обеспечивать достижение целей познающего субъекта. Таким образом, в уголовно-процессуальной теории отсутству-

¹⁷ Вывод основан на изучении материалов 125 уголовных дел о взяточничестве, рассмотренных судами города Москвы и Московской области за период с 2008 по 2018 г., выявленных методом случайной выборки, а также 250 материалов судебной практики Центрального, Приволжского, Южного и Сибирского федеральных округов Российской Федерации за период с 2006 по 2018 г., опубликованных в государственной автоматизированной системе «Правосудие», справочно-правовых системах «КонсультантПлюс», «Гарант».

¹⁸ Кони А. Ф. Избранные произведения : Воспоминания : в 2 т. 2-е изд., доп. М. : Госюриздат, 1959. Т. 2. С. 401.

ют препятствия для вывода о недопустимости возбуждения исключительно на основании аудио- и видеозаписи, однако совершенно очевидно, что для массового внедрения подобного механизма с учетом высоких стандартов международного законодательства необходима регламентация требований к содержанию таких аудио- и видеозаписей. Реализация курса на цифровизацию процессуальной деятельности требует систематизации судебной практики и выработки руководящих начал использования технических средств в уголовном судопроизводстве.

2. С учетом необходимости переосмысления соотношения понятий основания для возбуждения уголовного дела и оснований для предъявления обвинения в уголовном судопроизводстве существуют ли предпосылки для упрощения процедуры доказывания при наличии аудио- и видеозаписи преступления и при полном признании лица в совершении инкриминируемого деяния?

В условиях современного уголовно-процессуального законодательства ответ должен быть отрицательным. Назначение уголовного судопроизводства состоит в защите интересов как лиц, пострадавших от незаконной деятельности, так и лиц, привлекаемых к уголовной ответственности. Субъекты, осуществляющие предварительное расследование, помещены в главу УПК РФ, посвященную регламентации полномочий стороны обвинения, т.е. законодатель определил их в качестве процессуальных оппонентов подозреваемого, обвиняемого. Однако, как справедливо отметила В. А. Лазарева, наделение исключительными полномочиями на сбор доказательств на досудебной стадии, а также необходимость обеспечения защиты прав участников уголовного судопроизводства «роднит» процессуальный статус суда и лица, осуществляющего предварительное расследование¹⁹. Несмотря на то что современный УПК РФ не унаследовал изложенный в совет-

ском уголовном судопроизводстве принцип объективной истины, следователь и дознаватель в процессе доказывания обязаны устанавливать обстоятельства как подтверждающие, так и опровергающие виновность подозреваемого, обвиняемого в совершении преступления. Таким образом, формирование убежденности управомоченного лица в доказанности преступления возможно только в условиях преодоления презумпции невиновности совокупностью доказательств.

В данном случае необходимо ограничивать «основное» доказательство, содержание и информативность которого существенно влияет на возможность установления обстоятельств уголовного дела, от единственного доказательства, положенного в основу обвинения. Если в первом случае возникает каркас дальнейшей познавательной деятельности в рамках уголовного судопроизводства, то во втором фактически имеет место игнорирование одного из базовых элементов процедуры доказывания — проверки доказательств. Статья 87 УПК РФ определяет комплекс действий, необходимых для корректной проверки доказательств: сопоставление с другими доказательствами, имеющимися в деле; установление источников доказательств; получение иных доказательств, подтверждающих или опровергающих проверяемое доказательство. При этом вопрос наличия признательных показаний становится несущественным, поскольку, как справедливо отмечено в п. 17 постановления Пленума Верховного Суда РФ от 29.11.2016 № 55 «О судебном приговоре»²⁰, признание вины, не подтвержденное совокупностью других доказательств, приводит к невозможности постановления обвинительного приговора.

Особое значение подобные рассуждения приобретают в условиях применения особого порядка судебного разбирательства. Согласно судебной статистике упрощенная форма судебного разбирательства в 2017 г. применялась

¹⁹ Лазарева В. А. Российский следователь: судья или инквизитор? // Уголовное судопроизводство. 2018. № 4. С. 6—11.

²⁰ Российская газета. № 277. 07.12.2016.

в 64,5 % (598 938 из 914 982) уголовных дел. В 2016 г. эта цифра составила 65,8 % (636 448 из 967 159)²¹. При этом ученые отмечают высокую степень «устойчивости» таких приговоров при дальнейшей процедуре обжалования. В подобных условиях стремление к упрощению процедуры доказывания должно рассматриваться как недопустимое уменьшение процессуальных гарантий прав личности.

От того, получится ли у представителей науки и практики адекватно и вовремя отреагировать на эти и многие другие вопросы, порождаемые достижениями современной науки и изменениями структуры общественных отношений, во многом зависит не только успешная цифровизация системы государственного управления, но и будущее направление развития уголовного судопроизводства.

БИБЛИОГРАФИЯ

1. Гарусов А. В. О некоторых проблемах оценки показаний лиц, заинтересованных в исходе уголовного дела // Вестник Санкт-Петербургского университета МВД России. — 2016. — № 2 (70). — С. 60—64.
2. Завидов Б. Д., Кузнецов Н. П. Проблемы доказательств и доказывания в уголовном судопроизводстве // СПС «КонсультантПлюс», 2004.
3. Кони А. Ф. Избранные произведения : Воспоминания : в 2 т. / — 2-е изд., доп. — М. : Госюриздат, 1959. — Т. 2. — 536 с.
4. Курс уголовного процесса / под ред. д. ю. н., проф. Л. В. Головки. — 2-е изд., испр. — М. : Статут, 2017. — 1280 с.
5. Лазарева В. А. Российский следователь: судья или инквизитор? // Уголовное судопроизводство. — 2018. — № 4. — С. 6—11.
6. Левченко О. В. Классификация доказательств в уголовном процессе // Вестник Оренбургского государственного университета. — 2013. — № 3 (152). — С. 111—114.
7. Основы уголовного судопроизводства : учебник для бакалавров / М. В. Бубчикова, В. А. Давыдов, В. В. Ершов [и др.] ; под ред. В. А. Давыдова, В. В. Ершова. — М. : РГУП, 2017. — 444 с.
8. Россинский С. Б. Правовые условия применения мер уголовно-процессуального пресечения приводят к поспешности и необоснованности обвинения // Законы России: опыт, анализ, практика. — 2018. — № 5. — С. 30—36.
9. Рыжаков А. П. Показания свидетеля — самый распространенный вид доказательств. Комментарий к статье 79 УПК РФ // СПС «КонсультантПлюс», 2006.
10. Теория доказательств в советском уголовном процессе / отв. ред. Н. В. Жогин. — Изд. 2-е, испр. и доп. — М. : Юрид. лит., 1973. — 736 с.
11. Уголовно-процессуальное право (Уголовный процесс) : учебник для студентов вузов, обучающихся по направлению подготовки «Юриспруденция» / под ред. А. В. Ендольцевой, О. В. Химичевой, Е. Н. Клециной. — М. : Юнити-Дана: Закон и право, 2015. — 727 с.
12. Уголовно-процессуальное право Российской Федерации : учебник / отв. ред. П. А. Лупинская, Л. А. Воскобитова. — 4-е изд., перераб. и доп. — М. : Норма: Инфра-М, 2018. — 1008 с.
13. Уголовно-процессуальное право Российской Федерации : учебник для вузов / под общ. ред. Г. М. Резника. — М. : Юрайт, 2013. — 859 с.
14. Уголовно-процессуальный кодекс Российской Федерации. Главы 1—32.1. Постатейный научно-практический комментарий / Е. К. Антонович, Е. А. Артамонова, Д. П. Великий [и др.] ; отв. ред. Л. А. Воскобитова. — М. : Редакция «Российской газеты», 2015. — Вып. III—IV. — 912 с.

²¹ Основные статистические показатели деятельности судов общей юрисдикции за 2017 год // Официальный сайт Судебного департамента при Верховном Суде РФ. URL: <http://www.cdep.ru>.

15. Уголовный процесс : учебник / А. В. Смирнов, К. Б. Калиновский ; под общ. ред. проф. А. В. Смирнова. — 4-е изд., перераб. и доп. — М. : Кнорус, 2008. — 704 с.
16. Уголовный процесс : учебник для бакалавриата юридических вузов / О. И. Андреева [и др.] ; под ред. О. И. Андреевой, А. Д. Назарова, Н. Г. Стойко и А. Г. Тузова. — Ростов н/Д : Феникс, 2015. — 445 с.

Материал поступил в редакцию 6 мая 2019 г.

THE RATIO OF THE GROUNDS FOR INITIATING A CRIMINAL CASE AND THE GROUNDS FOR CHARGES IN CONDITIONS OF DIGITIZATION OF CRIMINAL PROCEEDINGS²²

OBIDIN Kirill Vyacheslavovich, International Law Office «Glinka, Rubinstein and Partners», Intern
obidinkirill.2018@gmail.com
107045, Russia, Moscow, Sretenskiy bulvar, d. 5

Abstract. *The proliferation and active use of technical means of audio and video recording in the process of identifying and proving certain types of crimes leads to the need to rethink the correlation of certain theoretical concepts. The paper analyzes similar elements and differences in the grounds for initiating a criminal case and the grounds for accusation. Attention is drawn to the convergence of the content of these concepts in the conditions of the spread of digital technologies in criminal proceedings. It is suggested that the use of audio and video recordings in a cognitive procedure has a significant effect on the inner conviction of the investigator and the inquiry officer when making procedural decisions. The possibility of initiating a criminal case is analyzed solely on the basis of audio and video. The author states his point of view on the inadmissibility of simplifying the procedure for establishment of evidence in cases of audio and video recordings, along with confessions, since in this case there is a violation of the basic foundations of cognitive activity in criminal proceedings.*

Keywords: *digitalization, audio and video recordings, grounds for criminal prosecution, grounds for bringing charges, proof, sufficiency, bribery.*

REFERENCES (TRANSLITERATION)

1. Garusov A. V. O nekotoryh problemah ocenki pokazanij lic, zainteresovannyh v iskhode ugovnogo dela // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. — 2016. — № 2 (70). — S. 60—64.
2. Zavidov B. D., Kuznecov N. P. Problemy dokazatel'stv i dokazyvaniya v ugovnom sudoproizvodstve // SPS «Konsul'tantPlyus», 2004.
3. Koni A. F. Izbrannye proizvedeniya : Vospominaniya : v 2 t. / — 2-e izd., dop. — M. : Gosyurizdat, 1959. — T. 2. — 536 с.
4. Kurs ugovnogo processa / pod red. d. yu. n., prof. L. V. Golovko. — 2-e izd., ispr. — M. : Statut, 2017. — 1280 s.
5. Lazareva V. A. Rossijskij sledovatel': sud'ya ili inkvizitor? // Ugovnoe sudoproizvodstvo. — 2018. — № 4. — S. 6—11.
6. Levchenko O. V. Klassifikaciya dokazatel'stv v ugovnom processe // Vestnik Orenburgskogo gosudarstvennogo universiteta. — 2013. — № 3 (152). — S. 111—114.

²² The study is carried out with the financial support of the Russian Foundation for Basic Research, Research Project No. 18-29-16041.MK.

7. Osnovy ugolovnogogo sudoproizvodstva : uchebnik dlya bakalavrov / M. V. Bubchikova, V. A. Davydov, V. V. Ershov [i dr.] ; pod red. V. A. Davydova, V. V. Ershova. — M. : RGUP, 2017. — 444 s.
8. Rossinskij S. B. Pravovye usloviya primeneniya mer ugolovno-processual'nogo presecheniya privodyat k pospeshnosti i neobosnovannosti obvineniya // Zakony Rossii: opyt, analiz, praktika. — 2018. — № 5. — S. 30—36.
9. Ryzhakov A. P. Pokazaniya svidetelya — samyj rasprostranennyj vid dokazatel'stv. Kommentarij k stat'e 79 UPK RF // SPS «Konsul'tantPlyus», 2006.
10. Teoriya dokazatel'stv v sovetskom ugolovnom processe / otv. red. N. V. Zhogin. — Izd. 2-e, ispr. i dop. — M. : Yurid. lit., 1973. — 736 s.
11. Ugolovno-processual'noe pravo (Ugolovnyj process) : uchebnik dlya studentov vuzov, obuchayushchihsya po napravleniyu podgotovki «Yurisprudenciya» / pod red. A. V. Endol'cevoj, O. V. Himichevoj, E. N. Kleshchinoj. — M. : Yuniti-Dana: Zakon i pravo, 2015. — 727 s.
12. Ugolovno-processual'noe pravo Rossijskoj Federacii : uchebnik / otv. red. P. A. Lupinskaya, L. A. Voskobitova. — 4-e izd., pererab. i dop. — M. : Norma: Infra-M, 2018. — 1008 s.
13. Ugolovno-processual'noe pravo Rossijskoj Federacii : uchebnik dlya vuzov / pod obshch. red. G. M. Reznika. — M. : Yurajt, 2013. — 859 s.
14. Ugolovno-processual'nyj kodeks Rossijskoj Federacii. Glavy 1—32.1. Postatejnyj nauchno-prakticheskij kommentarij / E. K. Antonovich, E. A. Artamonova, D. P. Velikij [i dr.] ; otv. red. L. A. Voskobitova. — M. : Redakciya «Rossijskoj gazety», 2015. — Vyp. III—IV. — 912 s.
15. Ugolovnyj process : uchebnik / A. V. Smirnov, K. B. Kalinovskij ; pod obshch. red. prof. A. V. Smirnova. — 4-e izd., pererab. i dop. — M. : Knorus, 2008. — 704 s.
16. Ugolovnyj process : uchebnik dlya bakalavriata yuridicheskikh vuzov / O. I. Andreeva [i dr.] ; pod red. O. I. Andreevoj, A. D. Nazarova, N. G. Stojko i A. G. Tuzova. — Rostov n/D : Feniks, 2015. — 445 s.

Информационная (цифровая) экосистема адвокатуры в контексте экосистемы цифровой экономики России¹

Аннотация. В статье дан обзор общих признаков «экологического подхода» в сфере информатизации. Определено соотношение и взаимосвязь понятий «цифровая экосистема», «экосистема программного обеспечения», «экосистема цифровой экономики», «экосистема информационного общества», «информационная (цифровая) экосистема адвокатуры».

Определено место информационной (цифровой) экосистемы адвокатуры как части экосистемы цифровой экономики России и экосистемы информационного общества. Описана структура и дана общая характеристика информационной (цифровой) экосистемы адвокатуры.

Ключевые слова: адвокатура, экосистема цифровой экономики, экосистема информационного общества, цифровая экосистема, информационная (цифровая) экосистема адвокатуры.

DOI: 10.17803/1994-1471.2019.103.6.156-166

Термин «экосистема» все чаще употребляется применительно к IT-сфере.

Одной из целей программы «Цифровая экономика Российской Федерации», утвержденной распоряжением Правительства РФ от 28 июля 2017 г. № 1632-р (далее — Программа цифровой экономики), является создание экосистемы цифровой экономики Российской Федерации, в которой данные в цифровой форме являются

ключевым фактором производства во всех сферах социально-экономической деятельности и в которой обеспечено эффективное взаимодействие, включая трансграничное, бизнеса, научно-образовательного сообщества, государства и граждан.

Речь идет не просто о необходимости внедрения и развития информационных технологий, но именно о создании экосистемы цифровой экономики.

¹ Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16170 «Концептуальные основы нормативного регулирования единой цифровой среды адвокатуры России».

© Гаврилов С. Н., Володина С. И., 2019

* Гаврилов Сергей Николаевич, кандидат юридических наук, кандидат исторических наук, адвокат Lab.kafadv@msal.ru

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

** Володина Светлана Игоревна, кандидат юридических наук, адвокат, доцент кафедры адвокатуры Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)

s.volodina@bk.ru

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

По нашему мнению, построение упорядоченного информационного пространства (цифровой среды) адвокатской корпорации должно осуществляться не просто как механистичное накопление и использование информационных продуктов, пусть и современных, а на системной основе и при соответствующем уровне качества таких продуктов.

В таком случае должен быть применен подход, при котором проектирование архитектуры информационных систем, выбор технологий и платформ, разработка программного обеспечения, подбор необходимого оборудования и решение других вопросов формирования информационной (цифровой) экосистемы адвокатуры следует рассматривать как создание части цифровой экономики страны при сохранении и реализации принципа независимости адвокатуры как института гражданского общества.

В литературе такой подход называют «экологическим», а создаваемые цифровые продукты рассматриваются в виде некоей экосистемы².

1. «Естественное» vs «искусственное». Обращает на себя внимание определенная метафоричность понятия «экосистема», применяемого в контексте информационных технологий.

Полагаем, что употребление данного понятия, изначально связанного с природным (биологическим) миром, применительно к ИТ-сфере лишь фиксирует аналогию многих процессов, происходящих в столь различных средах (в естественно-природной и искусственно созданной). В настоящее время наблюдается «растительный поворот» в гуманитаристике и технологиях.

В числе свойств естественных экосистем возможно назвать такие, как разнообразие, сложность, целостность, взаимосвязанность и взаи-

мозависимость организмов и среды, адаптивность, самовоспроизводимость, саморегуляция, устойчивость, равновесие, эмерджентность³, эволюционирование, сукцессия⁴.

В своей сущности естественные экосистемы имеют кибернетическую природу. Обладая множеством внутренних механизмов, а также сетевых каналов, по которым идут потоки физических, химических и иных сигналов, экосистема живет. При этом естественные экосистемы — это системы не «алгоритмического уровня». Связи между элементами в них носят сложный, не всегда очевидный характер.

В литературе отмечалось, что «цифровые экосистемные модели основаны на естественных экосистемах, особенно они схожи в отношении аспектов, связанных с конкуренцией и сотрудничеством между различными субъектами»⁵. Вследствие этого и появился термин «экологический подход». Под ним, в частности, подразумевают методологию исследований программного обеспечения как целой (системной) части окружающей среды, рассматриваемой в форме экосистемы⁶.

Вот, например, какие признаки ИТ-продуктов выделяют в литературе, проводя аналогии между биологическими и информационными системами:

- изменение (развитие) — непереносимое свойство программ, обусловленное наличием обратных связей и связанное с законами эволюции программ;
- метасистема, в рамках которой развивается программа, включает продукты деятельности, процессы и организацию, содержит большое количество обратных связей, стабилизирующих внутренних механизмов, влия-

² См., например: *Гопоненко А. А., Исхакова А. Р.* Цифровые экосистемы программной инженерии // Международный студенческий научный вестник. 2018. № 5. URL: <https://eduherald.ru/ru/article/view?id=18782> (дата обращения: 31.12.2018).

³ Эмерджентность (от англ. emergent — неожиданно появляющийся) — новые, уникальные свойства экосистемы, возникающие в результате синергичного взаимодействия ее компонентов.

⁴ Сукцессия (от лат. *succesio* — преемственность, наследование) — последовательная закономерная смена одного биологического сообщества другим.

⁵ Цит. по: *Гопоненко А. А., Исхакова А. Р.* Указ. соч.

⁶ См.: *Гопоненко А. А., Исхакова А. Р.* Указ. соч.

ющих на процессы планирования, управления и повышения эффективности;
— эффективное планирование и обслуживание программы требует понимания ее места в метасистеме, а также взаимодействия как между элементами, так и внутри них⁷.

2. «Экосистема» и «информационные технологии». Употребление термина «экосистема» происходит в различных контекстах. Говорится, например, о «цифровой экосистеме», об «экосистеме программного обеспечения», «экологии программного обеспечения», наконец, об «экосистеме цифровой экономики» и «экосистеме информационного общества».

«Цифровая экосистема». Существуют различные подходы к определению понятия «цифровая экосистема». В частности, предлагаются следующие определения: «совокупность устройств, сервисов и технологий для удобного (с точки зрения простого обывателя) использования современных технологий в повседневной жизни» (В. Шендрик); «конвергенция трех сетей: ИТ-сети, социальной и обмена знаниями» (F. Nachira, P. Dini, A. A. Nicola); «домен кластерной среды, включающий биологические, экономические и цифровые виды» (E. Chang, M. West); «цифровые артефакты и инфраструктура передачи данных, их хранения и обработки, пользователей систем, включая социальные, экономические, политические, психологические и иные факторы, влияющие на осуществление взаимодействий» (H. Dong, F. K. Hussain, E. Chang)⁸ и др.

«Экосистема цифровой экономики». В соответствии с пп. «с» п. 4 Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы, утвержденной Указом Президента РФ от 09.05.2017 № 203 «О стра-

тегии развития информационного общества в Российской Федерации на 2017—2030 годы» (далее — Стратегия развития информационного общества в РФ), «экосистема цифровой экономики — партнерство организаций, обеспечивающее постоянное взаимодействие принадлежащих им технологических платформ, прикладных интернет-сервисов, аналитических систем, информационных систем органов государственной власти Российской Федерации, организаций и граждан».

В литературе используется и такое понятие, как **экосистема информационного общества**.

Если рассматривать информационную экосистему как некую часть окружающей среды, а информационное общество как «общество, в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан»⁹, то экосистему информационного общества возможно определить как информационную часть окружающей среды, интегрированную в информационное общество.

«Если говорить об экосистеме информационного общества, — отмечает Е. В. Петрова, — то изначально она, подобно любой экосистеме, строится как часть окружающей среды (в данном случае информационной) и лишь потом встраивается в структуру информационного общества. Конечно, это не означает, что существуют четко выделенные этапы «пока еще среда» и «теперь уже общество». Речь, скорее, идет о философско-методологическом анализе становления экосистемы информационного общества, при котором неизбежно приходится выделять некую логическую структуру и прибегать к определенной схематизации»¹⁰.

⁷ См.: Луцкий М., Сидоров Н. Программное обеспечение — экологический подход к исследованиям // Natural and Artificial Intelligence. SOFIA, 2010. С. 186.

⁸ Цит. по: Авдеенко Т. В., Алетдинова А. А. Цифровизация экономики на основе совершенствования экспертных систем управления знаниями // Цифровая экономика и Индустрия 4.0: теория и практика. Научно-технические ведомости СПбГПУ. Экономические науки. Т. 10. № 1. 2017. С. 11. URL: <http://elibrary.spbstu.ru/dl/2/j17-242.pdf/download/j17-242.pdf> (дата обращения: 30.12.2018).

⁹ См.: пп. «г» п. 4 Стратегии развития информационного общества в РФ.

¹⁰ См.: Петрова Е. В. Проблема диалектической взаимосвязи природного и социального аспектов адаптации человека в экосистеме информационного общества // Философия науки и техники. 2017. Т. 22. № 1. С. 79.

«Экосистема программного обеспечения». В. А. Хоменко в статье, опубликованной в 2011 г., сообщает, что обзор веб-сайтов ведущих производителей программного обеспечения показывает: большинство из них применяет понятие «экосистема программного обеспечения». При этом автор отмечает, что производители применяют этот термин «как есть», без теоретических базы или ссылок на соответствующие труды, и что лишь корпорация «Майкрософт» дает определение экосистемы программного обеспечения как совокупности взаимодействий и взаимных влияний организаций (государственных, учебных и коммерческих) и индивидуумов, работающих с программным обеспечением¹¹.

В настоящее время термин «экосистема программного обеспечения» часто используется в контексте совокупности процессов разработки, внедрения и эксплуатации программного обеспечения.

Экосистему программного обеспечения важно рассматривать не только как разработку, внедрение и эксплуатацию программного обеспечения с учетом экологических принципов и требований. Речь должна идти не только об использовании «зеленых технологий» (о экономии энергии, минимизации загрязнения окружающей среды и др.), но и об учете принципов и свойств естественных экосистем при разработке, внедрении и эксплуатации программного обеспечения с пониманием, что экосистема программного обеспечения «живет» во многом по аналогичным законам с биологической экосистемой.

Используется, например, такое понятие, как **экология программного обеспечения**, которое, впрочем, предполагает учет того же «зеленого подхода» при производстве и эксплуатации программного обеспечения.

Под экологическим подходом в программном обеспечении М. Луцкий и Н. Сидоров предлагают понимать методологию исследований, в основе которой лежит рассмотрение объекта как части окружающей среды в форме экосистемы, с учетом устойчивого развития¹².

Авторы отмечают, что применение экологических исследований в индустрии программного обеспечения показывает, что их распространение идет в трех основных направлениях:

- экологичность производства и использования технических объектов;
- использование ресурсосберегающих и безотходных производств программного обеспечения;
- применение к программному обеспечению экологических исследований (при рассмотрении его как экосистемы)¹³.

Именно третье направление, по нашему мнению, требует особого внимания и является наиболее важным при проектировании информационной (цифровой) экосистемы адвокатуры и разработке соответствующего программного обеспечения.

Основываясь на результатах работы зарубежных коллег¹⁴, авторы отмечают, что «при рассмотрении программных систем в контексте реального мира как экосистемы одна из основных задач исследований состоит в сборе, накоплении, систематизации и анализе информации о количественном характере взаимосвязей внутри программной системы, между программной системой и внешней средой для получения следующих результатов:

- оценка качества исследуемых программных систем — как экосистем;
- влияние причин изменений компонентов, источников и факторов воздействия;
- прогноз устойчивости программных систем как экосистем и допустимости изменений»¹⁵.

¹¹ Хоменко В. А. Экосистемы программного обеспечения // Вестник Нац. техн. ун-та «ХПИ»: сб. науч. тр. Темат. вып. : Новые решения в современных технологиях. Харьков : НТУ «ХПИ». 2011. № 23. С. 114—118. URL: <http://repository.kpi.kharkov.ua/handle/KhPI-Press/12822> (дата обращения: 04.01.2019).

¹² См.: Луцкий М., Сидоров Н. Указ. соч. С. 181.

Полагаем, что признак «устойчивого» развития может проявляться не во всех случаях. Ключевым является то, что объект рассматривается «как часть окружающей среды в форме экосистемы».

¹³ См.: Луцкий М., Сидоров Н. Указ. соч. С. 182.

¹⁴ Lehman M. M., Belady L. A. Program Evolution. Academic Press, 1985. 532 p.

¹⁵ См.: Луцкий М., Сидоров Н. Указ. соч. С. 187.

На основе зарубежных исследований (I. Berk, S. Jansen, L. Luinenburg и др.) Е. Ю. Журавлева дает следующее определение: «Экологии ПО (программного обеспечения) — коллекция систем программного обеспечения, которые развиваются и эволюционируют совместно в одной среде. Среды могут быть организационными (компания), социальными (комьюнити с открытыми источниками) или техническими (инфраструктуры)». Автор описывает контексты определения экологий программного обеспечения¹⁶.

Таким образом, понятие «экосистема», употребляемое в сфере информатизации, прижилось и применяется весьма активно.

3. Соотношение и взаимосвязь понятий «информационная (цифровая) экосистема адвокатуры», «цифровая экосистема», «экосистема цифровой экономики», «экосистема информационного общества», «экосистема программного обеспечения», «экология программного обеспечения». Совмещение «информационно-цифрового» и «экосистемного» аспектов, а также попытка рассмотреть информационную (цифровую) экосистему адвокатуры в контексте феноменов «цифровая экосистема», «экосистема программного обеспечения», «экосистема информационного общества» позволяет предложить следующую модельную конструкцию.

Информационная (цифровая) экосистема адвокатуры является:

- элементом экосистемы информационного общества;
- частью экосистемы цифровой экономики; и как совокупность программных продуктов и сетей (инфраструктуры):

- должна быть построена с учетом экосистемных принципов и с использованием свойств, присущих экосистемам;

- должна функционировать на основе экосистемных принципов, проявляя и используя свойства, присущие экосистемам.

Если исходить из правомерности проведения аналогий между экосистемами биологического и искусственного (информационного) характера, рассмотренные понятия («цифровая экосистема», «экосистема цифровой экономики», «экосистема информационного общества», «экосистема программного обеспечения»), позволяют выстроить некую иерархическую структуру видов информационных экосистем по аналогии с биологическими, где:

- «экосистема информационного общества» — например, в рамках России — это *мегаэкосистема*;

- экосистема цифровой экономики России — это *макроэкосистема (биом)*;

- «цифровая экосистема» — например, информационная (цифровая) экосистема адвокатуры — это *мезоэкосистема*;

- «экосистема программного обеспечения» — например, программного обеспечения информационной системы¹⁷ — это *микроэкосистема*.

При всей условности и схематичности приведенных нами аналогий предложенный подход позволяет в некоторой степени определить сущность и возможное место информационной (цифровой) экосистемы адвокатуры в информационном пространстве.

В таком случае информационная (цифровая) экосистема адвокатуры, отвечающая уровню мезоэкосистемы, содержит комплекс микро-

¹⁶ Журавлева Е. Ю. Экосистемы научного программного обеспечения: определения и взаимосвязи // Информационное общество: образование, наука, культура и технологии будущего. Труды XX Международной объединенной научной конференции «Интернет и современное общество», IMS-2017, Санкт-Петербург, 21—23 июня 2017 г.: сборник научных статей. Вып. 1. СПб.: Университет ИТМО, 2017. 192 с. URL: <https://openbooks.ifmo.ru/ru/file/6409/6409.pdf> (дата обращения: 13.01.2019).

¹⁷ «Информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств» (п. 3 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ (ред. от 18.12.2018) «Об информации, информационных технологиях и о защите информации»).

экосистем (например, информационных систем), является частью экосистемы цифровой экономики России как макроэкосистемы (биома) и экосистемы информационного общества как мегаэкосистемы.

4. Информационная (цифровая) экосистема адвокатуры и экосистема цифровой экономики России. Построение корпоративного информационного пространства адвокатуры при ее определенной корпоративной обособленности (своего рода самости) и сохранении принципа независимости адвокатуры предполагает определить место корпоративного информационного пространства в контексте общероссийского экономического информационного пространства.

Цифровая экономика, в соответствии с Программой цифровой экономики России, представлена следующими объектами, которые в своем тесном взаимодействии влияют на жизнь граждан и общества в целом:

- рынки и отрасли экономики (сферы деятельности), где осуществляется взаимодействие конкретных субъектов (поставщиков и потребителей товаров, работ и услуг);
- платформы и технологии, где формируются компетенции для развития рынков и отраслей экономики (сфер деятельности);
- среда, которая создает условия для развития платформ и технологий и эффективного взаимодействия субъектов рынков и отраслей экономики (сфер деятельности) и охватывает нормативное регулирование, информационную инфраструктуру, кадры и информационную безопасность.

Очевидно, что в предложенной интерпретации объектов экосистемы цифровой экономики России информационная (цифровая) экосистема адвокатуры, а также сама адвокатская корпорация (адвокатская деятельность) могут рассматриваться:

- как одна из государственно, экономически и публично значимых сфер деятельности по оказанию квалифицированной юридической помощи;
- как сфера практического применения платформ и технологий для развития компетенций в области адвокатской деятельности

и деятельности органов адвокатского самоуправления;

- как среда, которая создает условия для развития платформ и технологий и эффективного взаимодействия субъектов в области адвокатской деятельности (в деятельности по оказанию квалифицированной юридической помощи — с адвокатами, адвокатскими образованиями, органами адвокатского самоуправления во взаимодействии с правоохранительными и иными государственными органами в рамках процессуальных отношений; с иными органами и организациями в области защиты прав и законных интересов физических и юридических лиц).

Значимость адвокатуры для развития цифровой экономики и развития информационного общества состоит, по-нашему мнению, в следующем. Выполняя публично и государственно значимую функцию (являясь институтом, обеспечивающим конституционное право каждого на получение квалифицированной помощи, и институтом гражданского общества), адвокатура вместе с тем является значительной частью рынка юридических услуг — экономическим игроком. Таким образом, занимая уникальное место в системе публично-правовых и одновременно экономических отношений, адвокатура может стать моделью выстраивания системы информационного (цифрового) взаимодействия между гражданским обществом и государством в публично-правовой и экономической сферах.

Очевидно, что формирование «продвинутой» цифровой среды потребует не только одностороннего развития государственных сервисов в сфере госуслуг, электронного судопроизводства и т.п., с одной стороны, и развития, например, сегмента автоматизации адвокатской деятельности (Legaltech) информационной (цифровой) экосистемы адвокатуры — с другой. Следует планировать соответствующие интеграционные механизмы между участниками электронного взаимодействия.

На уровне сегмента информатизации деятельности органов адвокатского самоуправления в информационной (цифровой) экосистеме адвокатуры таким — интегрированным — сер-

висом может стать, например, автоматизированный процесс назначения адвокатов в качестве защитников в уголовном судопроизводстве. В данном случае речь идет не только об информатизации одной из уголовно-процессуальных функций, но и об обеспечении «бюджетной прозрачности» системы оплат адвокатам, участвовавшим в делах по назначению. Это требует информационной интеграции, например, с системами межведомственного электронного взаимодействия (СМЭВ) и (или) межведомственного электронного документооборота (МЭДО) путем разработки модулей сопряжения («шлюзов»). Данный проект весьма важен как для государства, так и для самой адвокатуры. В качестве одного из сервисов экосистемы он может стать драйвером построения информационной (цифровой) экосистемы адвокатуры в целом.

Программой цифровой экономики России предусматривается, что реализация отдельных направлений по отраслям экономики (сферам деятельности) будет осуществляться на основе дополнения Программы соответствующими разделами. Представляется возможным на основе проведенных (проводимых) исследований и реализованных (реализуемых) мероприятий по построению информационной (цифровой) экосистемы адвокатуры сформировать соответствующие стратегию и тактику развития экосистемы адвокатуры, а также разработать «дорожную карту», дополнить Программу цифровой экономики России соответствующим разделом.

5. Структура и общая характеристика информационной (цифровой) экосистемы адвокатуры. По мнению Т. В. Авдеенко и А. А. Алетдиновой, технологии и сервисы цифровых экосистем должны включать:

- развитую информационно-коммуникационную структуру;
- интерактивные сообщества, участвующие в предметно-ориентированных кластерах;
- информационные ресурсы;
- базы знаний;
- новые формы электронного взаимодействия;
- платформы для интеграции бизнеса, правительства и общества;
- цифровую среду.

По мнению авторов, расширяются функции всех сервисов: предоставление и использование цифровых услуг; электронная обработка всех видов информации; поддержка информационного взаимодействия; бизнес-аналитика на основе использования искусственного интеллекта; усиление междисциплинарного взаимодействия; поддержка различных потребностей в цифровой экосистеме; вовлечение в предметно-ориентированные кластеры¹⁸.

Согласно предлагаемой нами модели, информационная (цифровая) экосистема адвокатуры состоит из информационной среды, информационных систем, сервисов, ресурсов, сетей (инфраструктуры) и др., а также предполагает наличие оператора¹⁹ (в нашем случае — адвокатской корпорации), который должен являться не только и не столько потребителем технологических возможностей, сколько ключевым компонентом экосистемы.

Информационная (цифровая) экосистема адвокатуры рассматривается нами как распределенная корпоративная информационная система²⁰ адвокатуры России, использующая корпоративные и иные (некорпоративные) информационные ресурсы²¹ и информационные системы (интегрированная с ними), а также ин-

¹⁸ Авдеенко Т. В., Алетдинова А. А. Указ. соч. С. 12.

¹⁹ «Оператор информационной системы — гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных» (п. 12 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

²⁰ «Информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств» (п. 3 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

²¹ «Информационные ресурсы — отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных,

формационно-телекоммуникационная сеть²² (инфраструктура), которые эксплуатируются оператором²³ посредством использования информационных технологий²⁴, технических средств и в совокупности образуют цифровую корпоративную *мезоэкосистему*, входящую в цифровую *макроэкосистему* (биом) — экосистему цифровой экономики России и *мегаэкосистему* информационного общества.

Согласно предлагаемой нами модели, информационная (цифровая) экосистема адвокатуры:

а) структурно включает:

- оператора информационно-телекоммуникационного взаимодействия (адвокатская корпорация (члены корпорации, корпоративные структуры)), являющегося эксплуатантом корпоративной информационной системы (далее — КИС) и (или) иных элементов информационной (цифровой) экосистемы адвокатуры в рамках информационно-телекоммуникационного взаимодействия;
- КИС по типу ERP-систем (Enterprise Resource Planning System) или аналогичных ей;
- информационно-телекоммуникационные сети и иную инфраструктуру;

— иные (в том числе интегрированные) некорпоративные информационные системы, ресурсы, сети (инфраструктуру), используемые для цели и задач информационной (цифровой) экосистемы адвокатуры;

— информационную среду как совокупность информационных средств, воздействующих на адвокатскую корпорацию как оператора информационно-телекоммуникационного взаимодействия;

— внешних (некорпоративных) участников информационно-телекоммуникационного взаимодействия, включая операторов некорпоративных информационных систем (сервисов, ресурсов, сетей, инфраструктуры и др.);

б) характеризуется наличием:

— зрелой корпоративной культуры адвокатской корпорации как участника информационно-телекоммуникационного взаимодействия (оператора);

— развитой когнитивной базы адвокатской корпорации;

— безопасного программного обеспечения и сервисов²⁵, а также соответствия информационных систем и других элементов экосистемы требованиям Федерального закона

других информационных системах)» (п. 11 разд. 2 ГОСТ Р 43.0.2-2006 «Информационное обеспечение техники и операторской деятельности. Термины и определения»).

²² «Информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники» (п. 4 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

²³ Оператор в предлагаемой нами модели — адвокатская корпорация (члены корпорации, корпоративные структуры), являющаяся эксплуатантом информационной системы и (или) иных элементов информационной (цифровой) экосистемы адвокатуры в рамках информационно-телекоммуникационного взаимодействия.

²⁴ «Информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов» (п. 2 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

²⁵ Безопасное программное обеспечение и сервис — программное обеспечение и сервис, сертифицированные на соответствие требованиям к информационной безопасности, устанавливаемым федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, или федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации» (пп. «а» п. 4 Стратегии развития информационного общества в РФ).

- от 27.07.2006 № 152-ФЗ «О персональных данных» (с послед. изм. и доп.);
- развитой КИС (включая наличие необходимых, актуальных и достаточных корпоративных ресурсов; использование надежных, современных информационных технологий и технических средств (систем, подсистем, устройств, сервисов и др.);
 - необходимых, актуальных, достоверных и достаточных корпоративных и иных (в том числе некорпоративных) информационных ресурсов;
 - доступа и (или) эффективной интеграции с иными (в том числе некорпоративными) информационными системами, ресурсами, сетями, инфраструктурой для цели и задач информационной (цифровой) экосистемы адвокатуры;
- в) обладает свойствами** целостности, адаптивности, саморегуляции, устойчивости, развития (эволюционирования/сукцессии), синергии/эмерджентности;
- г) предполагает создание условий:**
- для создания корпоративных систем и механизмов, обеспечивающих совершенствование корпоративной культуры, включая формирование и развитие когнитивной базы адвокатской корпорации;
 - конвергенции (интеграции) трех сегментов (уровней) информационной (цифровой) экосистемы адвокатуры: 1) сегмента автоматизации адвокатской деятельности (Legaltech); 2) сегмента информатизации деятельности адвокатских образований; 3) сегмента информатизации деятельности органов адвокатского самоуправления (включая КИС в качестве основного компонента данного сегмента);
 - информационного сопровождения корпоративных функций и процессов, а также построения и функционирования различных сервисов (например, автоматизированного распределения дел по назначению, электронного документооборота);
 - совершенствования КИС;
 - доступа и (или) эффективной интеграции с иными некорпоративными информационными системами, ресурсами, сетями, инфраструктурой для цели и задач информационной (цифровой) экосистемы адвокатуры;
 - развития информационно-телекоммуникационных сетей и иной инфраструктуры;
 - применения совокупности информационных технологий и использования средств, которые интегрируют цифровые артефакты и при помощи инфраструктуры обеспечивают передачу данных, их хранение и обработку, а также сопровождение необходимых функций и процессов;
 - взаимодействия в информационной среде корпоративных и внешних участников (в частности, для интеграции в системах СМЭВ и МЭДО);
 - реализации иных задач для достижения цели информационной (цифровой) экосистемы адвокатуры.
- Оговоримся, что предложенная нами характеристика проектируемой информационной (цифровой) экосистемы адвокатуры является рабочей и дана в качестве исходной, предполагающей проведение специальных исследований, которые планируются нами в рамках проекта построения информационной (цифровой) экосистемы адвокатуры.
- При этом очевидно, что разработка и построение информационной (цифровой) экосистемы адвокатуры должны осуществляться на междисциплинарной основе с учетом культурологического, психологического, этико-правового, технологического и ряда других факторов, влияющих на осуществление информационно-телекоммуникационного взаимодействия.

БИБЛИОГРАФИЯ

1. Авдеенко Т. В., Алетдинова А. А. Цифровизация экономики на основе совершенствования экспертных систем управления знаниями // Цифровая экономика и Индустрия 4.0: теория и практика. Научно-технические ведомости СПб.ГПУ. Экономические науки. — 2017. — Т. 10. — № 1. — URL: <http://elibr.spbstu.ru/dl/2/j17-242.pdf/download/j17-242.pdf>.
2. Гопоненко А. А., Исхакова А. Р. Цифровые экосистемы программной инженерии // Международный студенческий научный вестник. — 2018. — № 5. — URL: <https://eduherald.ru/ru/article/view?id=18782>.
3. Журавлева Е. Ю. Экосистемы научного программного обеспечения: определения и взаимосвязи // Информационное общество: образование, наука, культура и технологии будущего. Труды XX Международной объединенной научной конференции «Интернет и современное общество», IMS-2017, Санкт-Петербург, 21—23 июня 2017 г.: сборник научных статей. — СПб.: Университет ИТМО, 2017. — Вып. 1. — 192 с. — URL: <https://openbooks.ifmo.ru/ru/file/6409/6409.pdf>.
4. Луцкий М., Сидоров Н. Программное обеспечение — экологический подход к исследованиям // Natural and Artificial Intelligence. — SOFIA, 2010.
5. Петрова Е. В. Проблема диалектической взаимосвязи природного и социального аспектов адаптации человека в экосистеме информационного общества // Философия науки и техники. — 2017. — Т. 22. — № 1.
6. Хоменко В. А. Экосистемы программного обеспечения // Вестник Нац. техн. ун-та «ХПИ»: сб. науч. тр. Темат. вып. : Новые решения в современных технологиях. — Харьков: НТУ «ХПИ». — 2011. — № 23. — С. 114—118. — URL: <http://repository.kpi.kharkov.ua/handle/KhPI-Press/12822>.
7. Briscoe G. and Wilde P. De. Digital Ecosystems: Evolving service-oriented architectures // Conference on Bio Inspired Models of Network, Information and Computing Systems. — IEEE Press, 2006.

Материал поступил в редакцию 6 мая 2019 г.

IT (DIGITAL) ECOSYSTEM OF THE ADVOCACY IN THE CONTEXT OF RUSSIAN DIGITAL ECONOMY ECOSYSTEM

GAVRILOV Sergey Nikolaevich, PhD in Law, PhD in History, Lawyer

Lab.kafadv@msal.ru

125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

VOLODINA Svetlana Igorevna, PhD in Law, Advocate, Associate Professor of the Department of Advocacy of the Kutafin Moscow State Law University (MSAL)

s.volodina@bk.ru

125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

Abstract. *The paper provides an overview of the general features of an «environmental approach» in the field of information. The relationship and interrelation of the concepts «digital ecosystem», «software ecosystem», «ecosystem of digital economy», «ecosystem of information society», «IT (digital) advocacy ecosystem» is defined. The importance of the IT (digital) ecosystem of the advocacy as a part of the ecosystem of the digital economy of Russia and the ecosystem of the information society has been determined. The author describes the structure and gives the general characteristic of the IT (digital) ecosystem of the advocacy.*

Keywords: *advocacy, digital economy ecosystem, information society ecosystem, digital ecosystem, IT (digital) advocacy ecosystem.*

²² The study has been carried out with the financial support of the Russian Fund of Basic Research within the framework of the scientific project No. 18-29-16170 «The Concept Foundations of the Normative Regulation of a Uniform Digital Environment of the Bar of Russia».

REFERENCES (TRANSLITERATION)

1. Avdeenko T. V., Aletdinova A. A. Cifrovizaciya ekonomiki na osnove sovershenstvovaniya ekspertnyh sistem upravleniya znaniyami // Cifrovaya ekonomika i Industriya 4.0: teoriya i praktika. Nauchno-tekhicheskie vedomosti SPb.GPU. Ekonomicheskie nauki. — 2017. — T. 10. — № 1. — URL: <http://elib.spbstu.ru/dl/2/j17-242.pdf/download/j17-242.pdf>.
2. Goponenko A. A., Iskhakova A. R. Cifrovye ekosistemy programmnoj inzhenerii // Mezhdunarodnyj studencheskij nauchnyj vestnik. — 2018. — № 5. — URL: <https://eduherald.ru/ru/article/view?id=18782>.
3. Zhuravleva E. Yu. Ekosistemy nauchnogo programmnoho obespecheniya: opredeleniya i vzaimosvyazi // Informacionnoe obshchestvo: obrazovanie, nauka, kul'tura i tekhnologii budushchego. Trudy XX Mezhdunarodnoj ob»edinennoj nauchnoj konferencii «Internet i sovremennoe obshchestvo», IMS-2017, Sankt-Peterburg, 21—23 iyunya 2017 g : sbornik nauchnyh statej. — SPb. : Universitet ITMO, 2017. — Vyp. 1. — 192 s. — URL: <https://openbooks.ifmo.ru/ru/file/6409/6409.pdf>.
4. Luckij M., Sidorov N. Programmnoe obespechenie — ekologicheskij podhod k issledovaniyam // Natural and Artificial Intelligence. — SOFIA, 2010.
5. Petrova E. V. Problema dialekticheskoy vzaimosvyazi prirodnogo i social'nogo aspektov adaptacii cheloveka v ekosisteme informacionnogo obshchestva // Filosofiya nauki i tekhniki. — 2017. — T. 22. — № 1.
6. Homenko V. A. Ekosistemy programmnoho obespecheniya // Vestnik Nac. tekhn. un-ta «HPI» : sb. nauch. tr. Temat. vyp. : Novye resheniya v sovremennyh tekhnologiyah. — Har'kov : NTU «HPI». — 2011. — № 23. — S. 114—118. — URL: <http://repository.kpi.kharkov.ua/handle/KhPI-Press/12822>.

КРИМИНАЛИСТИКА И КРИМИНОЛОГИЯ. СУДЕБНАЯ ЭКСПЕРТИЗА

Е. А. Антонян*,
И. И. Аминов**

Блокчейн-технологии в противодействии кибертерроризму¹

***Аннотация.** В статье современные технологии блокчейн названы революционным явлением, равным по значимости гениальному изобретению XX столетия — Интернету. Первоначально разработанные для цифровой валюты биткойна и запуска одноименной сети, технологии блокчейн создали платформу нового вида Интернета, повлияли на децентрализацию Сети по принципу распределенного реестра, стали использоваться во всевозможных разновидностях и сочетаниях для разнообразных целей, включая кибербезопасность.*

В статье утверждается, что применение технологии блокчейн для обеспечения кибербезопасности безгранично благодаря таким уникальным свойствам, как надежность, общедоступность, высокая адаптивность, экономическая эффективность, рентабельность. Использование блокчейн-технологий в целях борьбы с киберпреступностью, в том числе кибертерроризмом, может распространяться на контроль над финансовыми услугами, транспортной или любой другой отраслью. Однако рост криминальной активности с использованием технологий блокчейн будет также усиливаться, если правоохранительные органы не смогут технологически грамотно, с опережающими темпами обнаруживать эти развивающиеся центры, определять их действия и разрушать планы.

¹ Исследование выполнено при финансовой поддержки РФФИ в рамках научного проекта № 18-29-16175 «Блокчейн-технологии противодействия рискам кибертерроризма и киберэкстремизма: криминологическое-правовое исследование».

© Антонян Е. А., Аминов И. И., 2019

* Антонян Елена Александровна, доктор юридических наук, профессор, профессор кафедры криминологии и уголовно-исполнительного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)

antonuaa@yandex.ru

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

** Аминов Илья Исакович, кандидат юридических наук, кандидат психологических наук, доцент, доцент кафедры криминологии и уголовно-исполнительного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)

aminovii@mail.ru

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

Ключевые слова: цифровые трансформации, виртуальное пространство, технология, блокчейн, биткоин, децентрализация, анонимность, кибертерроризм, криптовалюта, киберугрозы, кибератаки, хеширование, шифровка информации.

DOI: 10.17803/1994-1471.2019.103.6.167-177

Жизнь современного общества отмечена стремительным развитием компьютерных технологий, масштабным ростом числа пользователей Интернета, всеобщей киберинтеграцией. Цифровая трансформация охватила такие основополагающие сферы деятельности, как государственное управление, экономика, политика, законодательство, судопроизводство, бизнес, менеджмент, образование и наука. В виртуальное пространство переместились общение, обучение, банковские операции, покупки, хранение информации и многое другое. Одна из главных ролей в этих процессах принадлежит технологии блокчейн в различных ее разновидностях и сочетаниях.

Несомненно, блокчейн — революционное явление, по значимости сопоставимое с гениальным изобретением XX столетия — Интернетом. Первоначально (2008 г.) технология блокчейн (англ. blockchain, block chain — цепочка блоков) была разработана для цифровой валюты биткоин (от англ. bit — бит, т.е. единица измерения информации, и coin — монета), называемой «цифровом золотом», и запуска сети Биткоин². Термин «блокчейн» означал полностью реплицированную распределенную базу (реестр) данных и относился к транзакциям в различных криптовалютах. Впоследствии технология цепочек блоков была распространена и на иные взаимосвязанные информационные блоки³. В настоящее время разрабатываются и реализуются новые варианты и виды применения блокчейна. Так, взрыв распространения цифровой информации привел к тому, что технология блокчейн создала платформу нового

вида Интернета и способствовала появлению децентрализованных сервисов. В отличие от централизованного подхода, новые услуги основаны на децентрализованной распределенной сети, которая может использоваться для различных целей, включая кибербезопасность.

Технология блокчейн основывается на том, что у каждого пользователя базы данных, основанной на блокчейне, хранится ее полная копия (правило распределенного реестра). После любого внесения изменений в данную базу новая информация синхронизируется на компьютерах всех пользователей. Таким образом, отсутствует центральный депозитарий, который хранит базу данных, следит за ее актуальностью, надежно защищает от атак, поскольку потеря базы на одном и даже нескольких компьютерах никак не повлияет на сохранность информации: такие же копии хранятся у других пользователей. А если таких виртуальных хранилищ тысячи, миллионы или десятки миллионов, то такую базу данных можно считать относительно неуязвимой.

Посредством блокчейна информация через распределенные записи децентрализуется, последовательно хешируется (от англ. hashing — перемешивание, преобразование) и зашифровывается, что делает практически невозможным для злоумышленников ее выявление и осмысление⁴. Каждый раз, когда в распределенный реестр включаются новые данные, создается следующий блок, содержащий криптографически сформированный ключ, служащий для разблокировки произведенной записи.

Специфическим свойством технологии блокчейн является то, что внесение изменений

² Галушкин А. А. К вопросу о кибертерроризме и киберпреступности // Вестник Российского университета дружбы народов. Серия : Юридические науки. 2014. № 2. С. 44—49.

³ Генкин А. С., Михеев А. А. Блокчейн. Как это работает и что ждет нас завтра. М. : Альпина Паблицер, 2017. 592 с.

⁴ Luff C. Cybersecurity and the future of blockchain technology // URL: <http://www.gingermaypr.com/cybersecurity-blockchain-technology.htm> (дата обращения: 15.02.2019).

в базу данных (реестр) окончательно и необратимо: информация о транзакции запечатывается в виртуальный блок, который после регистрации действия синхронизируется со всеми копиями реестра. При этом блоки последовательно выстраиваются в цепочку. Таким образом, технология блокчейн гарантированно избавляет реестр от подделок и мошеннических действий в силу того, что внесение изменений возможно только в той части, которой владеет пользователь реестра, а также обеспечивает полную прозрачность операций в реестре и прослеживаемость всей цепочки блоков от момента создания. Срок хранения данных в реестре блокчейн неограничен, то есть информация может храниться фактически вечно⁵.

На сегодняшний день блокчейн в наибольшей степени востребован в финансовом секторе (создание цифровых валют, совершение транзакций, обмен и хранение финансовой информации). Он получил прикладное использование и в других сферах, таких как смарт-контракты, регистрация публичных записей (регистрация права собственности на недвижимое имущество, лицензирование, создание и ликвидация организаций, записи актов гражданского состояния, выдача цифровых удостоверений личности, водительских прав, электронных медицинских карт и т.д.).

Вместе с тем блокчейн имеет и свои слабые места. В частности, при сосредоточении более чем 51 % узловых точек (вычислительных мощностей) в рамках одной замкнутой цепочки (пула) она приобретает абсолютный контроль над процессом регистрации сделок в блокчейне, сводя на нет основополагающее свойство блокчейна — децентрализацию реестров данных⁶. Кроме того, блокчейн не так уже анонимен, как это принято считать. Система блокчей-

нов служит виртуальной записью всех транзакций в сети, доступной для всех пользователей блокчейна. «Прозрачность» и общедоступность блокчейна означают, что любой пользователь, имеющий достаточный уровень компьютерной грамотности, способен отслеживать цифровые следы анонимных трейдеров. В связи с этим для повышения безопасности и анонимности блокчейн часто используется в даркнете — теневом Интернете (от англ. DarkNet — темная сеть) — с анонимным программным обеспечением The Onion Router (TOR), представляющим собой систему прокси-серверов, позволяющих тайно входить в Интернет, сохранять анонимность при посещении сайтов, обмене мгновенными сообщениями, работе с приложениями⁷ и т.д.

Кроме предоставления очевидных преимуществ и нового качества жизни, тотальная цифровизация повлекла за собой не только масштабную зависимость общества от информационных технологий, но и возникновение киберпреступности, а также наиболее разрушительных ее форм — кибертерроризма и киберэкстремизма. Интернет реализовался в создании киберпространства, в котором террористы и экстремисты могут быстро и анонимно осуществлять обширный обмен информацией, беспрепятственно совершать коммуникации и наносить атаки на объекты, представляющие для них ценность.

Сегодня в Сети активно проводят работу такие террористические группы, как ХАМАС, Хезболла, египетская Аль-Гамаа аль-Исламия, Курдская рабочая партия, Аль-Каида, Исламское государство Ирака и Леванта (ИГИЛ), а также сотни других. Воинствующие радикальные организации рассматривают Интернет как идеальную арену для незаконной деятельности из-за крайне недостаточного законодательного регу-

⁵ Кумуков М. Ш. Технология блокчейн: новые вызовы и возможности в системе мер по ПОД/ФТ (противодействие отмыванию денег и/или финансированию терроризма) // Ленинградский юридический журнал. 2018. № 2. С. 144—154.

⁶ Allen J. How Blockchain Could Help Fight Cybercrime // URL: <https://techacute.com/how-blockchain-could-help-fight-cybercrime/> (дата обращения: 15.02.2019).

⁷ Malik N. How Criminals And Terrorists Use Cryptocurrency: And How To Stop It // URL: <https://www.google.ru/search?ie=UTF-8&hl=ru&q=blockchain%20against%20cyberterrorism%20and%20cyber-extremism> (дата обращения: 15.02.2019).

лирования отношений в киберсети, беспрепятственного распространения потока бесплатной информации, легкого доступа в онлайн-пространство практически из любой точки мира.

Сверхвозможности для кибертеррористов создали даркнет, а также неконтролируемые фискальной системой цифровые расчеты, виртуальную логистику, мгновенный обмен сообщениями, анонимность транзакций. Киберпреступники пользуются децентрализованной организацией теневого Интернета для проведения незаконных транзакций, для получения платежей от жертв вымогательств и для отмыwania доходов. В целях осуществления преступных намерений террористические организации активно используют цифровые технологии — блокчейн, искусственный интеллект (англ. artificial intelligence, AI), большие данные (big data), дополненная и виртуальная реальность, роботизация, 3D-печать и др. Интернет используется ими для безопасной связи, сбора информации, распространения пропаганды, нанесения кибератак на базы данных и критические информационные инфраструктуры, ведения психологической и развязывания реальной войны, вербовки, рекрутинга бойцов и сочувствующих.

Излюбленной валютой для рынков даркнета стал биткоин. В теневом Интернете кибертеррористы за криптовалюту могут покупать все, что угодно, включая наркотики, лекарства, оружие, киллеров, анонимно участвовать в торговле людьми, травле, запугивании, провоцировании и осуществлении террористических и экстремистских актов. Недавнее исследование показало, что почти половина всех операций с биткоинами являются незаконными⁸. Рост криминальной активности с использованием криптовалют, вероятно, будет усиливаться, если правоохранительные органы не смогут технологически обнаруживать эти развивающиеся рынки, определять их действия и разрушать планы.

В данном контексте следует кратко, в самом общем виде, пояснить, что понимается под ки-

бертерроризмом и в чем его отличительные черты. На этот счет существует много мнений, подходов, терминов, какого-то однозначного и общепринятого определения кибертерроризму пока не дано. Это, по нашему мнению, стало серьезным упущением, поскольку необходимо доподлинно знать и конкретно понимать все явления, с которыми приходится сталкиваться и бороться.

Под кибертерроризмом довольно часто понимают киберпреступность, однако явным отличием кибертерроризма является политический (и (или) идеологический, религиозно-этнический, социальный) мотив. Киберпреступность же нацелена исключительно на финансовую выгоду.

На основании анализа и обобщения российских и зарубежных источников⁹ можно заключить, что *кибертерроризм* — это преднамеренная, идеологически и политически мотивированная преступная деятельность, осуществляемая в киберпространстве посредством цифровых технологий и направленная против информации, компьютерных систем, компьютерных программ и баз данных, а также объектов критической информационной инфраструктуры, которая создает угрозу жизни или здоровью людей или наступления других тяжких последствий, если такие действия были содеяны с целью нарушения общественной безопасности, запугивания населения и органов власти, достижения преступных намерений, провокации военного конфликта. При этом террористические кибератаки могут быть направлены на объекты как виртуальной среды, так и реальной действительности.

Особо отметим, что Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»¹⁰ в ч. 4 ст. 2 определяет, что компьютерная атака — это целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты

⁸ Allman K. The dark side of the Bitcoin // Law Society of NSW Journal. Iss. 42 (Mar 2018). URL: <https://search.informit.com.au/documentSummary;dn=436097450333633;res=IELHSS> (дата обращения: 15.02.2019).

⁹ Галушкин А. А. Указ. соч.

¹⁰ СЗ РФ. 2017. № 31 (ч. I). Ст. 4736.

критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

В свою очередь, Федеральным законом от 26.07.2017 № 194-ФЗ в Уголовный кодекс РФ¹¹ была введена ст. 274.1, определяющая наказания за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Отличительной особенностью кибертеррористических актов (атак) является то, что они, как правило, нацелены на критически важные системы инфраструктуры, чтобы отключить, например, водоочистную станцию, вызвать региональное отключение электроэнергии, нарушить работу трубопровода, нефтеперерабатывающего завода или объектов транспорта. По данным Комиссии по защите критической инфраструктуры США, возможные цели кибертерроризма включают банковскую индустрию, военные объекты, электростанции, центры управления воздушным движением и системы водоснабжения¹². Подобные кибератаки могут разрушить крупные города, сорвать политические выборы в органы власти, обвалить финансовую систему страны, вызвать кризис общественного здравоохранения, вызвать перебои с поставками продовольствия, поставить под угрозу общественную и государственную безопасность, а также вызвать массовую панику и гибель людей.

Операции кибертеррора могут осуществляться с применением разнообразных кибертехнологий, среди которых:

— различные виды *вредоносного программного обеспечения (ПО)*, например X-Agent, X-Tunnel, PsExec и другие программы для удаленного выполнения команд, передачи файлов, шпионажа за нажатыми клавиша-

ми, уничтожения следов своего пребывания в Сети, периодического вычищения журналов событий и изменения атрибутов времени, изменения файлов;

- *расширенные длительные угрозы (Advanced persistent threat, APT)* — это сложные и концентрированные сетевые атаки, в результате которых террористы получают доступ в корпоративную сеть и остаются там незамеченными в течение длительного периода с целью кражи данных, не нанося ущерб непосредственно сети или организации. Как правило, APT атакует целевые организации в секторах с ценной информацией, таких как национальная оборона, производство и финансовая индустрия;
- *вредоносные вирусы, компьютерные «черви» и системы контроля* за программным обеспечением объектов критической инфраструктуры (водоснабжение, транспортные системы, электросети, военные системы, экологические комплексы и т.д.);
- *DoS-атаки* (от англ. Denial of Service — «отказ в обслуживании») и *DDoS-атаки* (от англ. Distributed Denial of Service — «распределенный отказ в обслуживании»), которые искусно наносятся террористами-хакерами для отключения корпоративных систем и сетей. Часто проводятся в рамках киберэкстракции (от англ. Cyber Extortion — «кибервымогательство, кибершантаж»);
- *взлом и кража особо важных данных (Hacking and theft of critical data)* государственных органов, учреждений и предприятий;
- *атака вымогателей (Attak Ransomware)*, которые держат компьютерные системы в заложниках, пока жертвы не заплатят выкуп;
- *фишинговые атаки* (от англ. fishing — «рыбная ловля, выуживание») — самый распространенный тип кибератак, представляющих собой попытки киберпреступников собирать информацию от жертв по электронной почте,

¹¹ Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СЗ РФ. 1996. № 25. Ст. 2954.

¹² Nakamoto Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Pp. 2—3 ; Rouse M. Cyberterrorism // URL: <https://searchsecurity.techtarget.com/definition/cyberterrorism> (дата обращения: 15.02.2019).

которую они затем могут использовать для доступа к системам или для кражи личных данных жертв.

Для тайного общения в Интернете при планировании действий и координации атак террористическими организациями, например Аль-Каидой, все чаще применяются зашифрованные коммуникационные платформы Telegram или Signal. Джихадисты для распространения идеологической пропаганды предпочитают Twitter и Facebook. Для обмена сообщениями киберэкстремисты активно используют программы и приложения WhatsApp, Threema, Kik, Wickr и SureSpot¹³.

Такие программы, как Google.Карты, способны предоставлять чрезвычайно важную для террористов информацию о расположении конкретных населенных пунктов или объектов, находить возможные точки входа в места, где планируются террористические атаки, а также рассматривать пути безопасного отхода и эвакуации. Потенциальные террористы в даркнете могут найти практически любой учебный материал: инструкции по созданию самодельных зажигательных и взрывных устройств, похищению людей и содержанию заложников, шантажу и запугиванию жертв. Есть даже руководства о том, как эффективно избежать онлайн-контроля со стороны антитеррористических групп.

Технологическая трансформация, запуск теневого Интернета и активное применение террористическими организациями цифровых технологий способствовали проявлению в современной онлайн-террористической деятельности новых опасных тенденций: 1) неуклонный и масштабный рост кибертерроризма; 2) целевое распространение идеологической и инструктивной информации на конкретную и наиболее восприимчивую аудиторию; 3) всемерная поддержка и поощрение приверженцев-одиночек¹⁴.

В последнее десятилетие благодаря Интернету и применению цифровых технологий оперативное планирование террористов стало более децентрализованным, изолированным и технологичным. Киберпространство имеет трансграничный характер, поэтому в случае совершения кибертеррористического акта трудно установить место нахождения террористов. Расположение компьютера, с помощью которого совершается террористический акт, крайне редко совпадает с местом расположения объекта посягательства и последствий деяния. Кроме того, технологическую проблему составляет сохранность следов совершения преступления и, соответственно, процесс розыска его исполнителей, что существенно снижает шансы их обнаружить и обезвредить. Остаются неясными ответы на вопросы: переместятся ли террористические атаки в киберпространство и сократится ли число реальных террористических актов (взрывы, поджоги, расстрелы, захваты заложников, наезды транспортных средств на людей и т.п.) или же терроризм останется таким же насильственным и физически выраженным?

Транснациональный характер кибертерроризма обуславливает тесное взаимодействие правоохранительных органов и специалистов в области IT-технологий разных стран. В целях обеспечения обмена результатами финансовой разведки и информацией, касающейся преступного использования цифровых валют, в частности финансирования кибертерроризма, в 2016 г. Европол, Интерпол и Базельский институт управления создали совместное подразделение по борьбе с отмыванием денег, специализирующееся на цифровых валютах. В задачи группы входят сбор и анализ информации о преступном использовании криптовалют, расследование хранения доходов, полученных преступным путем, организация ежегодных семинаров и встреч представителей трех ведомств

¹³ Is technology helping or hindering the fight against terrorism? // Dis-patch News & Politics, Science & Tech. December 15. 2017. URL: <https://wp.nyu.edu/dispatch/2017/12/15/is-technology-helping-or-hindering-the-fight-against-terrorism/> (дата обращения: 15.02.2019).

¹⁴ Is technology helping or hindering the fight against terrorism?

и других учреждений, а также создание сети специалистов по биткоин-преступности¹⁵. При поддержке Европола в июле 2017 г. были закрыты два крупнейших даркнет-маркета AlphaBay и Hansa Market, что стало результатом крупной международной операции, в которой принимали участие США, Канада, Таиланд, Голландия, Великобритания, Франция, Литва, а также представители Европола, ФБР и Управления по борьбе с наркотиками США¹⁶.

Очевидно, что для того, чтобы предотвратить террористические угрозы и радикализацию в киберпространстве, правоохранные органы должны иметь возможность быть в технологическом отношении на шаг впереди киберкриминала. Изворотливость и профессионализм современных кибертеррористов, а также их фантастически возросшие технологические возможности требуют от правоохранных органов всего мира разработки адекватных механизмов противодействия кибертерроризму, стратегия борьбы с которым должна быть направлена на предупреждение и минимизацию угроз и рисков, порождаемых глобальной цифровизацией. Конечная цель такого подхода должна состоять в исключении любых возможностей для действий террористов как в реальном мире, так и в киберпространстве.

Блокчейн открывает новые сверхэффективные способы противостояния кибератакам различными способами, одним из которых является надежная защита данных от взлома, кражи или уничтожения ценной информации. Если при взломе традиционной централизованной системы хакер за один вход может получить доступ ко всем тысячам объектов, то при взломе децентрализованной блокчейн-системы киберпреступники могут получить до-

ступ только к одному фрагменту, что делает их действия более трудоемкими, так как придется многократно взламывать базу, чтобы получить полную информацию. В свою очередь, у служб безопасности и правоохранительных органов появляется дополнительное время для выявления источника опасности и устранения угрозы¹⁷.

Возможность предотвращения кибератак заложена в самом принципе децентрализованной системы цепочки блоков, которая не только обеспечивает децентрализованную сеть для хранения информации, но и гарантирует ее безопасность за счет устойчивости к взлому хешированных и зашифрованных блоков. Сервер, основанный на блокчейне, может минимизировать атаки, создавая более разветвленную сеть и распределяя контроль между различными пользователями. Наличие автоматических распределенных регистров и неизменной истории транзакций позволяет предотвращать кибератаки. Последовательное хеширование и шифровка информации позволяют сохранять целостность данных¹⁸.

Принцип безопасности распределенной сети может применяться и для защиты такой жизненно важной внешней инфраструктуры, как служба доменных имен (англ. domain name services, DNS) веб-сайтов компаний. В 2016 г. мощная кибератака на Twitter и Spotify продемонстрировала уязвимость текущей практики DNS, заключающейся в том, что ключ доступа хранится только на одном сервере, а его надежность строится на хешировании путем кодирования и криптографии. Сервер на основе распределенного блокчейн-реестра создает более широкую сеть ключей безопасности, что гарантированно минимизирует риск взлома или уничтожения системы¹⁹.

¹⁵ Europol and Interpol to fight cryptocurrency crime together // URL: <http://www.coinfox.info/news/6404-europol-and-interpol-to-fight-cryptocurrency-crime-together> (дата обращения: 15.02.2019).

¹⁶ Galbraith K. The Emerging Threat of Cyberterrorism // Australian Outlook. 29 Jun 2018. URL: <http://www.internationalaffairs.org.au/australianoutlook/the-emerging-threat-of-cyberterrorism/> (дата обращения: 15.02.2019).

¹⁷ Blockchain Technology in the fight against Cybercrime / DISINI & DISINI // URL: <https://privacy.com.ph/dndfeature/blockchain-technology-in-the-fight-against-cybercrime/> (дата обращения: 15.02.2019).

¹⁸ Allen J. Op. cit.

¹⁹ Luff C. Op. cit.

Помимо защиты самих данных, блокчейн способен защитить от кибератак и процесс обмена информацией. Например, такие инструменты обмена мгновенными сообщениями, как Facebook Messenger или WhatsApp, хотя и оснащены системами безопасности, все же имеют слабые места. WhatsApp, несмотря на сквозное шифрование для защиты содержимого сообщений, сохраняет метаданные (информацию о том, с кем общается пользователь), которые обычно хранятся в отдельных системах, и велика вероятность, что хакеры их взломают. Технология цепочки блоков может децентрализовать сеть, разделить метаданные и гарантировать их совокупную недоступность.

Системы защиты интернет-серверов и информационно-коммуникационных систем должны не просто успевать совершенствоваться вслед за все более совершенными способами и методами исполнения актов кибертерроризма, а значительно опережать их.

Антитеррористические группы ряда стран уже применяют суперкомпьютеры с передовым программным обеспечением, в частности технологиями блокчейн, для оценки рисков возникновения кибертеррористических актов, накопления и анализа огромных объемов данных из глобального интернет-облака, выявления и распознавания схемы дислокации, перемещений и межличностных связей кибертеррористов, идентификации личности подозреваемых, установления контроля над их террористической деятельностью и передвижениями.

В 2016 г. британская полицейская контртеррористическая группа по борьбе с терроризмом (CTIRU) вывела из Интернета более 3 500 наименований вредных и незаконных материалов, включая пропагандистские фильмы, учебные пособия по терроризму, а также видеоролики и публикации, пропагандирующие или поддерживающие терроризм и экстремизм. Компания Palantir из Кремниевой долины на основе технологии блокчейн и анализа больших данных

создает и совершенствует программное обеспечение для отслеживания информации в целях борьбы с терроризмом для разведывательных, правоохранительных, частных детективных агентств, принося основателям компании доход в 1,5 млрд долл. США в год. Цифровая криминалистика также помогает следователям искать улики в цифровых отпечатках подозреваемых террористов, устанавливая их онлайн-активность, прослушивая разговоры и разыскивая покупки, чтобы найти доказательства преступных деяний. Специальное программное обеспечение, приобретенное у канадской компании Magnet Forensics, позволило ФБР США обнаружить улики на 30 электронных устройствах, принадлежащих террористам, ответственным за атаку во время Бостонского марафона (братья Царнаевы, 2013 г.).

Применение технологий блокчейн и продуктов на ее основе в противодействии кибертерроризму проводится, как правило, комплексно с другими супертехнологиями. Так, блокчейн в сочетании с искусственным интеллектом используется для фильтрации и идентификации важной информации, для поиска в огромных массивах данных.

На основе блокчейна разрабатывается программное обеспечение, способное выявлять и удалять террористический контент до того, как он получит массовое распространение. В 2018 г. Министерство внутренних дел Великобритании доложило о создании лондонской технологической компанией ASI Data Science комплексного инструмента искусственного интеллекта для обнаружения в 95 % террористического контента в онлайн-видео, с вероятностью выявления в 99,9 %²⁰.

Элементы технологии блокчейн присутствуют в программном обеспечении по выявлению и распознаванию лиц, в системах обнаружения взрывчатых веществ в транспортных средствах, роботах Packbots, способных проникать в чрезвычайно опасную для человека среду, и даже в высокотехнологичных лифтах, мгновенно до-

²⁰ Counter-terrorism strategy embraces tech, but warns of future extremist digital capabilities // URL: <https://www.itpro.co.uk/cyber-terrorism/31247/quantum-computing-could-help-fight-terrorism-says-uk-gov> (дата обращения: 15.02.2019).

ставляющих людей с верхних этажей небоскребов в вестибюль²¹.

Область применения технологии блокчейн в кибербезопасности безгранична благодаря таким его уникальным свойствам, как надежность, общедоступность, высокая адаптивность, экономическая эффективность и рентабельность. Использование блокчейна для борьбы с киберпреступностью может быть распространено на финансовые услуги, законодательство, транспортную отрасль или любую другую отрасль, требующую проверки третьей стороной.

Разумеется, в основе всех этих разработок и механизмов их применения в правоохранительной деятельности должно быть соответствующее законодательство, своевременно реагирующее на новые риски и угрозы, а также легализующее применение цифровых технологий. Представляется необходимым ввести в правовое поле деятельность провайдеров обмена цифровых валют, а также совершение сделок по купле-продаже не только токенов, но и криптовалюты, что позволит решить ряд первоочередных задач, таких как противодействие финансированию террористической деятельности и отмыванию доходов. Следует отметить, что практическая реализация требований об идентификации трейдеров является сложной из-за отсутствия прямого контакта с пользователем и отсутствия опробованных механизмов

идентификации применительно к криптовалютам.

Кроме того, законодательство должно регулярно совершенствовать уголовно-правовую оценку (квалификацию) киберпреступлений и киберправонарушений, вводить новые их виды, усиливать систему наказаний за кибертерроризм. Установить административные штрафы за такие правонарушения в виртуальной среде, как, например, неоднократный просмотр потокового террористического видеоконтента или пересылка файлов террористической и экстремистской направленности.

Таким образом, разработка высокотехнологичных цифровых механизмов противодействия кибертерроризму и объединение усилий государств всего мира является первоочередной задачей на современном этапе. Международному сообществу следует выработать единые для всех стран правила игры в сфере цифровых технологий, универсальный и общий для всех международный стандарт, который будет максимально учитывать интересы каждой страны. Должна быть улучшена трансграничная система обмена данными о киберугрозах. Вместе с тем меры безопасности не должны приниматься в ущерб технологическому прогрессу и инновациям. Свобода общения и коммуникаций, а также беспрепятственный обмен опытом и идеями в цифровую эпоху должны быть законодательно гарантированы.

БИБЛИОГРАФИЯ

1. *Галушкин А. А.* К вопросу о кибертерроризме и киберпреступности // Вестник Российского университета дружбы народов. Серия : Юридические науки. — 2014. — № 2. — С. 44—49.
2. *Генкин А. С., Михеев А. А.* Блокчейн. Как это работает и что ждет нас завтра. — М. : Альпина Паблицер, 2017. — 592 с.
3. *Кумуков М. Ш.* Технология блокчейн: новые вызовы и возможности в системе мер по ПОД/ФТ (противодействие отмыванию денег и/или финансированию терроризма) // Ленинградский юридический журнал. — 2018. — № 2. — С. 144—154.
4. *Allen J.* How Blockchain Could Help Fight Cybercrime // URL: <https://techacute.com/how-blockchain-could-help-fight-cybercrime/> (дата обращения: 15.02.2019).
5. *Allman K.* The dark side of the Bitcoin // Law Society of NSW Journal. — Iss. 42 (Mar 2018). — URL: <https://search.informit.com.au/documentSummary;dn=436097450333633;res=IELHSS> (дата обращения: 15.02.2019).

²¹ Is technology helping or hindering the fight against terrorism?

6. Blockchain Technology in the fight against Cybercrime / DISINI & DISINI // URL: <https://privacy.com.ph/dndfeature/blockchain-technology-in-the-fight-against-cybercrime/> (дата обращения: 15.02.2019).
7. Counter-terrorism strategy embraces tech, but warns of future extremist digital capabilities // URL: <https://www.itpro.co.uk/cyber-terrorism/31247/quantum-computing-could-help-fight-terrorism-says-uk-gov> (дата обращения: 15.02.2019).
8. Europol and Interpol to fight cryptocurrency crime together // URL: <http://www.coinfox.info/news/6404-europol-and-interpol-to-fight-cryptocurrency-crime-together> (дата обращения: 15.02.2019).
9. Galbraith K. The Emerging Threat of Cyberterrorism // Australian Outlook. — 29 Jun 2018. — URL: <http://www.internationalaffairs.org.au/australianoutlook/the-emerging-threat-of-cyberterrorism/> (дата обращения: 15.02.2019).
10. Is technology helping or hindering the fight against terrorism? // Dispatch News & Politics, Science & Tech. — December 15. — 2017. — URL: <https://wp.nyu.edu/dispatch/2017/12/15/is-technology-helping-or-hindering-the-fight-against-terrorism/> (дата обращения: 15.02.2019).
11. Luff C. Cybersecurity and the future of blockchain technology // URL: <http://www.gingermaypr.com/cybersecurity-blockchain-technology.htm> (дата обращения: 15.02.2019).
12. Malik N. How Criminals And Terrorists Use Cryptocurrency: And How To Stop It // URL: <https://www.google.ru/search?ie=UTF-8&hl=ru&q=blockchain%20against%20cyberterrorism%20and%20cyber-extremism> (дата обращения: 15.02.2019).
13. Nakamoto Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. — 2008.
14. Rouse M. Cyberterrorism // URL: <https://searchsecurity.techtarget.com/definition/cyberterrorism> (дата обращения: 15.02.2019).

Материал поступил в редакцию 6 мая 2019 г.

BLOCKCHAIN TECHNOLOGY IN COUNTERING CYBER TERRORISM²²

ANTONYAN Elena Aleksandrovna, Doctor of Law, Professor, Professor of the Department of Criminology and Penal Law of the Kutafin Moscow State Law University (MSAL)

antonyaa@yandex.ru

125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

AMINOV Ilya Isakovich, PhD in Law, PhD in Psychology, Docent, Associate Professor of the Department of Criminology and Penal Law of the Kutafin Moscow State University (MSAL)

aminovii@mail.ru

125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

Abstract. *In the paper, modern blockchain technologies are called a revolutionary phenomenon, equal in importance to the ingenious invention of the 20th century — the Internet. Originally developed for Bitcoin digital currency and launching the network of the same name, the blockchain technology created a platform for the new type of the Internet, influenced the decentralization of the Network according to the distributed registry principle, and began to be used in various types and combinations for various purposes, including cybersecurity.*

The paper argues that the use of blockchain technology to ensure cybersecurity is infinite due to such unique properties as reliability, accessibility, high adaptability, economic efficiency, profitability. The use of blockchain

²² The study is carried out with the financial support of the Russian Foundation for Basic Research, Research Project No. 18-29-16175 «Blockchain-technology for countering the risks of cyber-terrorism and cyber-extremism: criminological and legal research».

technologies to combat cybercrime, including cyberterrorism, may extend to control over financial services, transportation or any other industry. However, the growth of criminal activity using the blockchain technology will also be enhanced if the law enforcement agencies are not technologically competent, can detect these developing centers, determine their actions and destroy plans at a faster pace.

Keywords: *digital transformations, virtual space, technology, blockchain, bitcoin, decentralization, anonymity, cyber-terrorism, cryptocurrency, cyber threats, cyber attacks, hashing, encryption of information.*

REFERENCES (TRANSLITERATION)

1. Galushkin A. A. K voprosu o kiberterrorizme i kibereprestupnosti // Vestnik Rossijskogo universiteta družby narodov. Seriya : Yuridicheskie nauki. — 2014. — № 2. — S. 44—49.
2. Genkin A. S., Miheev A. A. Blokchejn. Kak eto rabotaet i chto zhdet nas zavtra. — M. : Al'pina Pablisher, 2017. — 592 s.
3. Kumukov M. Sh. Tekhnologiya blokchejn: novye vyzovy i vozmozhnosti v sisteme mer po POD/FT (protivodejstvie otmyvaniyu deneg i/ili finansirovaniyu terrorizma) // Leningradskij yuridicheskij zhurnal. — 2018. — № 2. — S. 144—154.

А. И. Семикаленова*,
И. А. Рядовский**

Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики¹

Аннотация. В статье проанализированы результаты изучения актуальной практики выявления, фиксации, сохранения и предваряющего судебную экспертизу исследования цифровых следов преступления. В качестве инструментария мониторинга следственной и оперативно-розыскной деятельности в данной области использовались личные беседы и опросы работников Следственного комитета Российской Федерации, следственных и оперативно-розыскных подразделений МВД России, сотрудников иных служб и ведомств, курсантов и студентов старших курсов высших учебных заведений, обучающихся по соответствующей специализации. Кроме того, были опрошены специалисты в области компьютерных информационных технологий как частного, так и государственного сектора, привлекаемые к проведению следственных действий и оперативно-розыскных мероприятий.

В статье представлены результаты данного исследования, выявлены актуальные проблемы уголовного судопроизводства, с которыми сталкиваются представители правоохранительных органов, расследующие преступления, сопряженные с информационно-компьютерными технологиями, при изъятии и фиксации компьютерной информации.

Ключевые слова: информационно-компьютерное обеспечение, компьютерное преступление, следственное действие, обыск, выемка, компьютерная информация, компьютерная сфера, информационно-цифровые технологии, информатизация, цифровые следы, интернет-мошенничества, удаленный доступ, допрос, осмотр, цифровые следы.

DOI: 10.17803/1994-1471.2019.103.6.178-185

¹ Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16003/18.

© Семикаленова А. И., Рядовский И. А., 2019

* Семикаленова Анастасия Игоревна, кандидат юридических наук, доцент кафедры судебных экспертиз Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
semiks@mail.ru

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

** Рядовский Игорь Анатольевич, руководитель отдела расследования компьютерных инцидентов АО «Лаборатория Касперского», почетный работник прокуратуры Российской Федерации

igor.ryadovsky@kaspersky.com

125212, Россия, г. Москва, Ленинградское ш., д. 39а, стр. 3

Информационными компьютерными технологиями пронизаны все сферы человеческой деятельности. Было бы странно ожидать, что при широком внедрении компьютеризации в общественные отношения сфера преступной деятельности оказалась бы незатронутой. Сегодня при совершении большого количества преступлений так или иначе используется компьютерное средство²: либо в качестве средства совершения преступления, как, например, при осуществлении незаконного доступа к защищаемой информации или интернет-мошенничествах, либо в качестве средства подготовки или сокрытия преступления — лжепредпринимательство, преступления в банковской сфере, распространение наркотических средств и др. Доля таких преступлений с каждым годом неуклонно растет, поэтому для их расследования необходимо существенное углубление и расширение знаний в области компьютерных технологий. Все чаще у следователей и оперативных сотрудников возникает необходимость привлечения лиц, обладающих специальными знаниями в данной области.

Особенно показательным в части распространности компьютерных технологий (в самом широком смысле) в качестве средств и орудий совершения преступлений стал 2018 г., в течение которого, согласно результатам опросов специалистов по информационной безопасности, впервые доля их участия по делам так называемых традиционных видов преступлений превысила количество дел о преступлениях в сфере компьютерной информации в 1,5 раза. При этом в абсолютных цифрах количество следственных действий и оперативно-розыскных мероприятий по делам о преступлениях в сфере компьютерной информации, в которых участвовали опрошенные специалисты, также возросло. Этот факт подтверждает тезис о всестороннем

проникновении информационных технологий в преступную сферу.

В ходе мониторинга следственной и оперативно-розыскной практики проведены опросы и анкетирования специалистов в области IT-технологий, которые показали, что сегодня, помимо участия в расследовании преступлений, сопряженных с неправомерным доступом к компьютерной информации, а также с разработкой и использованием вредоносных программ, указанные специалисты были наиболее востребованы при проведении следственных действий и оперативно-розыскных мероприятий по делам о традиционных видах мошенничества, незаконной организации азартных игр, незаконном обороте наркотических средств, об убийствах, о сообщениях о заведомо ложных актах терроризма. Если проанализировать общее число случаев участия в расследовании преступлений лиц, сведущих в рассматриваемой области знаний, то можно утверждать, что в последнее время возросла потребность следственных органов в дополнительных знаниях.

Особое место в применении специальных компьютерно-технических знаний в следственной и оперативно-розыскной практике занимает обнаружение и фиксация цифровых следов. К указанным следам авторы статьи совместно с профессором Е. Р. Россинской³ относят криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде, в процессе возникновения данной информации, ее обработки, хранения и передачи. Нами в течение последних двух лет было опрошено 100 следователей и 203 оперативных сотрудника. По мнению опрошенных респондентов, независимо от вида расследуемого преступления наиболее значимые мероприятия по обнаружению, сбору и фиксации таких следов связаны с выездами на место: будь

² Чекунов И. Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. 2012. № 1. С. 9—22 ; Нехорошев А. Б. Компьютерные преступления: квалификация, расследование, экспертиза / под ред. В. Н. Черкасова. Саратов : СЮИ МВД России, 2004. 372 с.

³ Россинская Е. Р., Рядовский И. А. Концепция цифровых следов в криминалистике // Аубакировские чтения : материалы междунар. науч.-практ. конференции (19 февраля 2019 г.). Алматы : Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының ҒЗЖРБЖҰБ, 2019. С. 6—8.

то доступ к рабочей станции подозреваемого в ходе обыска, получение компьютерной техники потерпевших в процессе выемки либо осмотр места происшествия — локальной компьютерной сети. На вопрос, к проведению каких следственных действий они привлекались наиболее часто, специалисты выделили:

- обыск (43 %);
- осмотр места происшествия (31 %);
- осмотр предметов, документов (16 %);
- выемка (10 %).

Федеральным законом от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности»⁴ в ст. 6 предусмотрены как специальные мероприятия — снятие информации с технических каналов связи и получение компьютерной информации, так и иные мероприятия, в ходе которых может быть произведен поиск, обнаружение и изъятие цифровых следов преступления. По сведениям, полученным от специалистов в области IT-технологий и оперативных сотрудников МВД России, наиболее часто специалисты привлекались к оперативно-розыскным мероприятиям:

- исследование (36 %);
- снятие информации с технических каналов связи (28 %);
- получение компьютерной информации (17 %);
- сбор образцов для исследования (12 %);
- оперативный эксперимент (7 %).

Анализ анкетных данных и данных опроса сотрудников следственных и оперативно-розыскных подразделений выявил проблему в сборе и фиксации цифровых следов при отображении их на удаленных компьютерных системах. Вызвана данная проблема тем, что уголовно-процессуальным законом не предусмотрены следственные действия по получению компьютерной информации с удаленных

компьютерных систем и сетей. В этой связи их приходится разрешать посредством поручения производства таких мероприятий органу, осуществляющему оперативно-розыскную деятельность. Вышеуказанные проблемы возникают при фиксации информации, расположенной на интернет-ресурсах, и часто касаются незаконного оборота наркотических средств, распространения порнографической или иной запрещенной к распространению на территории Российской Федерации информации, лжепредпринимательства.

Хотелось бы отметить, что несмотря на то, что ряд авторов уже писали о необходимости совершенствования действующего законодательства, регламентирующего расследование преступлений в сфере компьютерных технологий⁵, а также на то, что законодатель внес в УПК РФ⁶ статью 164.1, предусматривающую копирование интересующей следствие информации, все респонденты указывают на несовершенство уголовно-процессуального законодательства в части отсутствия в перечне следственных действий необходимых процессуальных инструментов, в рамках которых возможно удаленное получение компьютерной информации с компьютерных систем и сетей. По мнению респондентов, это особенно важно для расследования компьютерных преступлений, сопряженных с шифрованием информации. Поскольку компьютерные данные очень легко уничтожить либо зашифровать, преступники этим часто пользуются, чтобы скрыть доказательства от следствия. Они уделяют особое внимание мерам конспирации, для чего используют методы шифрования информации с использованием специализированных программных продуктов, типа TrueCrypt. Чтобы получить доступ к такой информации, содержащейся на изъятых копии компьютера, не-

⁴ Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (в редакции Федерального закона от 6 июля 2016 г. № 374-ФЗ) // СЗ РФ. 2016. № 28. Ст. 4558.

⁵ Торичко Р. С., Клишина Н. Е. Некоторые вопросы совершенствования действующего законодательства, регламентирующего расследование киберпреступлений // Вестник экономической безопасности. 2018. № 3. С. 179—184.

⁶ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 01.04.2019) // СЗ РФ. 2018. № 53. Ст. 8456.

обходимо ввести пароль либо использовать криптографический ключ, которыми следствие в большинстве случаев не располагает. Другой способ получения доступа к информации, имеющей значение для дела, — произвести удаленное подключение к компьютеру в процессе его работы. Данный способ сегодня может быть реализован только в рамках проведения оперативно-розыскных мероприятий по поручению следователя. Именно поэтому на наш вопрос, каковы главные задачи специалиста при производстве следственных действий и оперативно-розыскных мероприятий, 64 % респондентов ответили, что, помимо оказания содействия в поиске и обнаружении доказательств и применении технических средств, роль специалиста заключается в обеспечении доступа к компьютерным данным, имеющим значение для дела, которые при осмотре электронных носителей информации могут быть в зашифрованном виде.

Проанализировав уголовные дела и результаты опроса следственных и оперативных сотрудников, авторы пришли к выводу, что крайне важно привлекать лиц, обладающих специальными знаниями в области информационно-компьютерных технологий, уже на этапе планирования и подготовки следственных действий, связанных с поиском, обнаружением и фиксацией цифровых следов, — с целью получения компетентных разъяснений относительно доступности электронных доказательств и необходимости принятия мер к их сохранности. Однако обобщение результатов опроса показывает, что, несмотря на признаваемую всеми респондентами значимость данного этапа, наиболее распространенная и, наверное, общая и наиболее значительная ошибка — это отсутствие либо формальный подход к подготовке к проведению следственных действий и оперативно-розыскных мероприятий. Недаром на заведомо провокационный вопрос, каким образом они могли бы описать идеальное следственное действие или оперативно-розыскное мероприятие по сбору цифровых следов преступления, большинство респондентов ответили, что «идеальное мероприятие — это хорошо подготовленное мероприятие».

Из личных бесед с респондентами о показательных примерах из их правоприменительной практики можно сделать вывод, что нередко подготовка не учитывает специфики преступной деятельности в сфере компьютерной информации. Например, ошибка в месте производства обыска, когда квартира либо офис были установлены по входящему в помещение интернет-каналу провайдера, в сетевом трафике которого зафиксированы признаки противоправной активности, без проверки версии о компрометировании Wi-Fi-передатчика лицом, проживающим либо работающим в соседнем помещении. Отсутствие предварительного инструктажа всех участников мероприятия часто приводит к утрате криминалистически значимой информации уже в ходе производства обыска. Следователи и оперативные сотрудники, не имеющие опыта работы по таким делам, не всегда осознают, насколько легко подозреваемый может уничтожить информацию: закрыв крышку ноутбука либо выдернув силовую кабель, что свидетельствует об их недостаточных знаниях в области информационно-компьютерных технологий. Поскольку риск утраты компьютерной информации очень высок (гораздо выше, чем риск утраты традиционных доказательств), необходимо в первую очередь допустить к осмотру вычислительной техники специалистов, знакомых с правилами предосторожности.

В подтверждение такого вывода можно привести показательный пример из следственной практики, обстоятельства которого были изложены одним из респондентов в личной беседе. При подготовке производства обыска в офисном помещении, в котором были оборудованы компьютеризированные рабочие места участников организованной группы, осуществлявшей преступную деятельность в сфере компьютерной информации, следователем был разработан план осмотра и исследования этого помещения. Согласно плану исследование рабочих мест первоначально должен был провести криминалист с целью обнаружения и фиксации следов рук, после чего к осмотру компьютеров допускались специалисты в сфере компьютерной информации. Однако в результате обработки одного из ноутбуков дактилоскопическим порошком

на магнитную кисть среагировал встроенный в корпус датчик закрытия крышки, после чего операционная система переключила компьютер в энергосберегающий режим, следствием чего стала блокировка доступа к информации. Здесь явно прослеживается незнание специалистом-криминалистом особенностей компьютерной техники или элементарное их игнорирование, несоблюдение очередности работы с объектами на месте проведения следственного действия. При более тщательной подготовке обыска, разъяснении всем участникам особенностей работы с компьютерными объектами такого могло не произойти.

Опрос респондентов и личные беседы выявили еще одну проблему использования специальных знаний при поиске и фиксации цифровых следов преступления. Требования действующего законодательства обязывают лицо, производящее в ходе обыска либо выемки обнаружение, фиксацию и изъятие цифровых следов путем изъятия электронных носителей информации и копирования с них информации, привлекать к участию в следственном действии либо оперативно-розыскном мероприятии специалиста (ст. 164.1 УПК РФ). Подавляющее большинство опрошенных сотрудников следственных и оперативно-розыскных подразделений пояснили, что следуют этому требованию путем включения в состав следственно-оперативной группы криминалиста, как правило сотрудника соответствующего подразделения ЭКЦ МВД России, либо привлекают стороннего специалиста в сфере компьютерной техники. Причем, несмотря на отсутствие прямого указания на это в законе, изъятие и копирование электронных носителей информации в ходе осмотра места происшествия проводятся в большинстве случаев также с участием специалиста. Однако все опрошенные следственные и оперативные сотрудники отрицательно ответили на вопрос, понимали ли они, какой именно специализации и компетенции в области информационно-компьютерных технологий специалист им требуется.

В отличие от сотрудников следственных и оперативно-розыскных подразделений, опрошенные в ходе мониторинга специалисты пояс-

нили, что для производства мероприятий, нацеленных на поиск и фиксацию цифровых следов, следует привлекать специалистов, область познаний которых должна быть достаточно широка: в сфере компьютерных устройств и программирования, в области сетевого взаимодействия и эксплуатации сетевой инфраструктуры и т.п., либо следует привлекать нескольких специалистов с углубленными познаниями в определенных областях компьютерно-информационных технологий. При этом привлечение специалиста к проведению следственных действий по уголовным делам о преступлениях в сфере компьютерной информации требует от следователя понимания, каким требованиям должен соответствовать специалист, какими методиками обладать, какие технические средства использовать, чтобы обеспечить исчерпывающие меры к обнаружению и фиксации доказательств и исключить их утрату.

Существенные затруднения при определении источника, содержащего криминалистически значимую информацию, возникают при осмотре крупных компьютерных сетей, функционирование которых приостановить не представляется возможным ввиду непрерывного производственного процесса. Кроме того, изъятие с места происшествия всей компьютерной сети с целью производства судебной экспертизы не является целесообразным и разумным и в большинстве случаев технически возможным. В этом случае перед следователем стоит задача на месте происшествия выявить компьютерные устройства, подлежащие изъятию. При этом ни один из опрошенных представителей правоохранительных органов, за исключением сотрудников специализированных оперативно-розыскных подразделений, не смог ответить, что представляют из себя на уровне обработки компьютером перечисленные объекты и процессы операционных систем и как их изучение позволяет выполнить поставленную задачу.

Вместе с тем, как показывают результаты мониторинга, отсутствие даже базовых знаний об устройстве современных компьютеров, о функционировании их сетей, среде и циклах обращения компьютерной информации влияет на качество расследования преступлений,

совершенных с использованием информационно-компьютерных технологий, и может привести к невозможной утрате доказательств. Безусловно, привлеченный специалист, обладающий должной компетенцией, обязан оказать профессиональное содействие следователю в поиске и фиксации цифровых следов преступления⁷. Но, как свидетельствуют приведенные выше результаты мониторинга, для привлечения специалиста с соответствующей компетенцией от следователя требуется хотя бы минимальный образовательный уровень в сфере компьютерных технологий и обработки информации.

Одной из проблем сложившегося на сегодняшний день положения дел в следственной практике по поиску и фиксации цифровых следов преступления опрошенные сотрудники следственных и оперативно-розыскных подразделений называют отсутствие должной подготовки привлекаемых к мероприятиям специалистов в части отсутствия у них на месте необходимой криминалистической техники, позволяющей произвести изъятие и фиксацию на носителе-дубликате компьютерной информации в случае невозможности изъятия компьютерной системы, подлежащей исследованию, а в ряде случаев достаточных для проведения данных мероприятий знаний.

В личных беседах специалисты в области IT-технологий подтвердили наличие такой проблемы. Однако подобные ситуации характерны и в случае привлечения специалистов из сторонних, не связанных с обеспечением информационной безопасности организаций. Вместе с тем, по их мнению, обязанность удостовериться в наличии необходимых компетенций привлекаемого специалиста, в том числе выяснить, обладает ли специалист навыками работы с соответствующей криминалистической техникой, а также может ли обеспечить ее применение, лежит на лице, ведущем расследование, что становится невозможным без соответствующих специальных знаний у этого лица.

Опрошенные в ходе мониторинга специалисты также пояснили, что ни один перечень оборудования, инструментов и программного обеспечения, которые могут быть востребованы при изъятии компьютерной техники, обнаружении, осмотре и фиксации компьютерной информации, не может считаться исчерпывающим и должен составляться исходя из конкретных обстоятельств дела. Можно лишь говорить о необходимом минимуме, например:

- программы для снятия снимка (дампа) оперативной памяти (например, Belkasoft RAM Capturer, ProcDump);
- устройства, позволяющие изучать содержимое файловой системы в режиме «только чтение»;
- устройства-блокираторы для копирования НЖМД/SSD, исключающие возможность внесения изменений на исходный диск.

Итак, подводя итоги проведенного мониторинга, можно выделить следующие проблемные ситуации, связанные с поиском, фиксацией и исследованием цифровых следов преступления, приводящие к типичным следственным ошибкам:

- отсутствие подготовительных мероприятий;
- привлечение специалиста, не обладающего необходимой компетенцией;
- нарушение очередности криминалистических методов сбора доказательств, влекущее утрату компьютерной информации, имеющей существенное значение для дела;
- формальный подход к организации следственных действий и оперативно-розыскных мероприятий;
- отсутствие у лиц, проводящих следственные и оперативно-розыскные мероприятия, минимально необходимых знаний в области информационно-компьютерных технологий.

Основной же вывод: отсутствие системного, комплексного подхода в изучении темы расследования компьютерных преступлений в целом и обнаружения и фиксации цифровых следов в частности во многом вытекает

⁷ Чекунов И. Г., Рядовский И. А., Иванов М. А. [и др.]. Методические рекомендации по расследованию преступлений в сфере компьютерной информации : учебное пособие / под ред. И. Г. Чекунова. М. : Мос. ун-т МВД России имени В. Я. Кикотя, 2018. 106 с.

из недостаточной разработанности темы информационно-компьютерного обеспечения криминалистической деятельности⁸, развитие которой в дальнейшем позволит в значительной степени оптимизировать использование человеческих и технических ресурсов с целью быстрого и качественного раскрытия преступлений.

БИБЛИОГРАФИЯ

1. *Нехорошев А. Б.* Компьютерные преступления: квалификация, расследование, экспертиза / под ред. В. Н. Черкасова. — Саратов : СЮИ МВД России, 2004. — 372 с.
2. *Россинская Е. Р.* Концепция частной криминалистической теории «информационно-компьютерное обеспечение криминалистической деятельности» // Деятельность правоохранительных органов в современных условиях : сборник материалов XXIII Международной науч.-практ. конференции : в 2 т. — Иркутск : Восточно-Сибирский институт МВД РФ, 2018. — С. 113—118.
3. *Россинская Е. Р., Рядовский И. А.* Концепция цифровых следов в криминалистике // Аубакировские чтения : материалы международной научно-практической конференции (19 февраля 2019 г.). — Алматы : Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының ҒЗЖРБЖҰБ, 2019. — С. 6—8.
4. *Торичко Р. С., Клишина Н. Е.* Некоторые вопросы совершенствования действующего законодательства, регламентирующего расследование киберпреступлений // Вестник экономической безопасности. — 2018. — № 3. — С. 179—184.
5. *Чекунов И. Г.* Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений // Право и кибербезопасность. — 2012. — № 1. — С. 9—22.
6. *Чекунов И. Г., Рядовский И. А., Иванов М. А.* [и др.]. Методические рекомендации по расследованию преступлений в сфере компьютерной информации : учебное пособие / под ред. И. Г. Чекунова. — М. : Московский университет МВД России имени В. Я. Кикотя, 2018. — 106 с.

Материал поступил в редакцию 6 мая 2019 г.

⁸ *Россинская Е. Р.* Концепция частной криминалистической теории «информационно-компьютерное обеспечение криминалистической деятельности» // Деятельность правоохранительных органов в современных условиях : сборник материалов XXIII Междунар. науч.-практ. конференции : в 2 т. Иркутск : Восточно-Сибирский институт МВД РФ, 2018. С. 113—118.

THE USE OF SPECIAL KNOWLEDGE IN DETECTING AND FIXING DIGITAL TRACES: ANALYSIS OF MODERN PRACTICE⁹

SEMIKALENOVA Anastasia Igorevna, PhD in Law, Associate Professor of the Department of Forensic Examination of the Kutafin Moscow State Law University (MSAL)
semiks@mail.ru
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

RYADOVSKIY Igor Anatolievich, Head of Computer Investigation Department, Kaspersky Lab JSC, Honorary Prosecutor of the Russian Federation
igor.ryadovsky@kaspersky.com
125212, Russia, Moscow, Leningradskoye Shosse, d. 39a, str. 3

Abstract. *The paper analyzes the results of studying the current practice of identifying, fixing, preserving and anticipating the forensic examination of the study of digital traces of crime. As a toolkit for monitoring investigative and operational investigative activities in this area, there were applied personal conversations and surveys of employees of the Investigative Committee of the Russian Federation, investigative and operational search units of the Ministry of the Interior of Russia, employees of other services and departments, students of the relevant specialization. In addition, experts in the field of computer information technologies from both the private and public sector, involved in investigative actions and operational search activities were interviewed. The paper presents the results of this study, identifying current problems of criminal justice, faced by law enforcement officials investigating crimes involving information and computer technology, while seizing and recording computer information.*

Keywords: *information and computer software, computer crime, investigative action, search, seizure, computer information, computer sphere, information digital technologies, informatization, digital traces, Internet fraud, remote access, interrogation, inspection, digital traces.*

REFERENCES (TRANSLITERATION)

1. Nekhoroshev A. B. Komp'yuternye prestupleniya: kvalifikaciya, rassledovanie, ekspertiza / pod red. V. N. Cherkasova. — Saratov : SYul MVD Rossii, 2004. — 372 s.
2. Rossinskaya E. R. Konceptiya chastnoj kriminalisticheskoy teorii «informacionno-komp'yuternoe obespechenie kriminalisticheskoy deyatel'nosti» // Deyatel'nost' pravoohranitel'nyh organov v sovremennyh usloviyah : sbornik materialov XXIII Mezhdunarodnoj nauch.-prakt. konferencii : v 2 t. — Irkutsk : Vostochno-Sibirskij institut MVD RF, 2018. — S. 113—118.
3. Rossinskaya E. R., Ryadovskij I. A. Konceptiya cifrovyh sledov v kriminalistike // Aubakirovskie chteniya : materialy mezhdunarodnoj nauchno-prakticheskoy konferencii (19 fevralya 2019 g.). — Almaty : Qazaqstan Respublikasy IIM M. Esbolatov atynday Almaty akademiyasynuq FZzhRBZhYB, 2019. — S. 6—8.
4. Torichko R. S., Klishina N. E. Nekotorye voprosy sovershenstvovaniya dejstvuyushchego zakonodatel'stva, reglamentiruyushchego rassledovanie kiberprestuplenij // Vestnik ekonomicheskoy bezopasnosti. — 2018. — № 3. — С. 179—184.
5. Chekunov I. G. Sovremennye kiberugrozy. Ugolovno pravovaya i kriminologicheskaya klassifikaciya i kvalifikaciya kiberprestuplenij // Pravo i kiberbezopasnost'. — 2012. — № 1. — S. 9—22.
6. Chekunov I. G., Ryadovskij I. A., Ivanov M. A. [i dr.]. Metodicheskie rekomendacii po rassledovaniyu prestuplenij v sfere komp'yuternoj informacii : uchebnoe posobie / pod red. I. G. Chekunova. — M. : Moskovskij universitet MVD Rossii imeni V. Ya. Kikotya, 2018. — 106 s.

⁹ The study is carried out with the financial support of the Russian Foundation for Basic Research, Research Project No. 18- 29- 16003/18.

ИНТЕГРАЦИОННОЕ ПРАВО

А. Г. Барабашев*,
Д. В. Пономарева**

Защита персональных данных и научно-исследовательская деятельность: опыт правового регулирования ЕС¹

Аннотация. Правовое регулирование использования персональных данных играет значительную роль в обеспечении качества научных исследований. Регламент Европейского парламента и Совета ЕС № 2016/679 от 27 апреля 2016 г. «О защите прав физических лиц в отношении обработки персональных данных и о свободе перемещения таких данных, отменяющий Директиву 95/46/ЕС» ставит своей целью унификацию норм, регламентирующих защиту прав человека на неприкосновенность частной жизни, как на территории ЕС, так и, при определенных условиях, за его пределами. Это новелла, введенная Регламентом в правовое поле ЕС, служит дополнением и обновлением *acquis communautaire*, достигнутых в рамках Директивы 95/46/ЕС о защите персональных данных. Регламент устанавливает как общие правила, применимые к любому виду обработки персональных данных, так и специальные правила, применимые к анализу отдельных категорий персональных данных, таких как информация, полученная в ходе клинических исследований. В данной статье представлен обзор новых норм (действующих с мая 2018 г.), регламентирующих аспекты обработки персональных данных в контексте научно-исследовательской деятельности (персональные данные о здоровье, генетическая, биометрическая информация и т.д.).

Ключевые слова: Европейский Союз, защита персональных данных, биометрическая информация, генетическая информация, компьютерная безопасность.

DOI: 10.17803/1994-1471.2019.103.6.186-194

¹ Статья подготовлена в рамках гранта РФФИ 18-29-15022 мк «Способы, модели и проблемы регулирования и охраны субъективных прав в области получения, использования, распространения и защиты результатов научной деятельности и научной информации».

© Барабашев А. Г., Пономарева Д. В., 2019

* *Барабашев Александр Георгиевич*, кандидат юридических наук, доцент кафедры интеграционного и европейского права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

** *Пономарева Дарья Владимировна*, кандидат юридических наук, преподаватель кафедры практической юриспруденции Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

ВВЕДЕНИЕ

Результатом длительного и интенсивного реформирования законодательства о персональных данных в ЕС стало принятие Регламента № 2016/679 Европейского парламента и Совета ЕС от 27 апреля 2016 г. «О защите прав физических лиц в отношении обработки персональных данных и о свободе перемещения таких данных, отменяющий Директиву 95/46/ЕС». Принятием указанного Регламента Европейский Союз подтвердил свою приверженность защите основных прав и свобод человека, в частности связанных с защитой неприкосновенности частной жизни, в том числе право на защиту данных личного характера, закрепленное в Хартии Европейского Союза об основных правах и в рамках Договора о функционировании Европейского Союза, а также готовность Союза ускорить достижение цели создания единого внутреннего рынка, где беспрепятственное перемещение персональных данных имеет основополагающее значение для развития экономических отношений.

Регламент не только унифицирует правила для всех государств-членов, тем самым нивелируя нормативные противоречия, которые существовали между государствами-членами в период действия Директивы 95/46/ЕС о защите данных, но и предоставляет субъектам правоотношений возможность осуществлять полноценный контроль над своими персональными данными в условиях сетевого общества. Целью Регламента является создание устойчивых мер по защите персональных данных. Будучи преемником Директивы 95/46/ЕС, Регламент внес ряд важных изменений в сферу правового регулирования защиты персональных данных (в особенности, в части прав субъектов и процедур). Регламент, как и предшествующая ему Директива 95/46/ЕС, применяется к контролерам обработки данных, действующим в государственном и частном секторах. Он также разграничивает категории персональных данных, строго регламентируя их обработку. В частности, это касается особых категорий персональных данных (данные о здоровье, генетические и биометрические данные) ввиду возникновения рисков возможного нарушения прав и свобод человека. Регламент,

как и Директива 95/46/ЕС, рассматривает сферу научных исследований как специфическую область обработки персональных данных, где необходимость установления равновесия между свободой личности и свободной научного исследования вызывает массу этических проблем. В рамках Регламента вводится новый подход к обработке персональных данных, основанный на учете рисков и призванный облегчить в каждом конкретном случае выявление проблем и принятие соответствующих мер по защите данных.

В указанной статье мы предлагаем рассмотреть следующие вопросы: 1) обновленные общие принципы защиты персональных данных при проведении научных исследований; 2) новые процедуры обработки; 3) конкретные положения, касающиеся прав субъектов данных в контексте исследований и 4) новые возможности для дальнейшего регулирования защиты данных в области научных исследований.

ОБЩИЕ ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЛАСТИ НАУЧНЫХ ИССЛЕДОВАНИЙ

Регламент поддерживает подход, принятый в рамках предшествовавшей ему Директивы, устанавливая общие принципы, которые должны соблюдаться в любом контексте обработки персональных данных, в том числе в исследовательских целях, и независимо от их вида, в частности для обработки особой категории персональных данных.

Основные общие принципы полностью заимствованы из Директивы 95/46/ЕС. Согласно ст. 5 Регламента обработка персональных данных осуществляется в соответствии с требованиями законности, справедливости и транспарентности в отношении субъекта данных; сбор осуществляется для определенных, явных и законных целей, при этом данные не должны обрабатываться несовместимым с этими целями способом; данные должны быть адекватными, соответствующими и должны ограничиваться целями, для достижения которых они обрабатываются; данные должны быть точными и, при необходимости, актуальными; разумные меры должны

быть приняты для гарантии того, что неточные персональные данные будут незамедлительно удалены или исправлены; данные должны храниться в форме, позволяющей идентифицировать субъектов данных, не дольше, чем это необходимо для целей, во исполнение которых персональные данные проходят обработку.

Регламент дополняет вышеупомянутые принципы, закрепляя в ст. 5 три относительно новых дополнительных принципа. Первый касается соблюдения целостности данных и их конфиденциальности. Этот принцип требует, чтобы персональные данные обрабатывались с учетом обеспечения надлежащей безопасности, включая защиту от несанкционированной или незаконной обработки и от случайной потери, уничтожения или повреждения, с использованием соответствующих технических или организационных мер. Этот принцип находит свое отражение не только в соблюдении требований профессиональной этики научных исследований, таких как обеспечение научной и исследовательской интеграции, но и в технических мерах, в частности в использовании: методов кодирования; защищенных от внешних угроз серверов; закрытой системы обработки данных и др. Указанный принцип особенно важен в контексте исследований, когда речь идет о потенциально большом объеме конфиденциальных данных и когда качество данных имеет основополагающее значение для обеспечения надежности результатов исследований, их полезности и проверяемости.

Вторым принципом, частично вытекающим из положений Директивы 95/46/ЕС, является принцип подотчетности. В соответствии с ним контролер обработки данных является ответственным лицом, демонстрирующим соблюдение общих принципов обработки данных, изложенных выше. Это предполагает ведение контролером обработки персональных данных или его представителем четкой и защищенной отчетности в отношении любого вида деятельности по обработке данных, осуществляемой под их ответственность. В рамках научных исследований такая отчетность может вестись в виде архива, который будет храниться в течение определенного периода времени. В статье 30

Регламента указывается минимальный объем информации, подлежащей учету (хранению) в рамках такого рода письменной отчетности. Каждый контролер и (или) обработчик обязуется сотрудничать с контролирующим органом и предоставлять отчетные сведения по запросу таких органов.

Третий общий принцип тесно связан с необходимостью создания на уровне ЕС устойчивой системы защиты данных путем использования специальных технологий, повышающих конфиденциальность при проведении операций по обработке и на протяжении всего периода существования данных. В данном случае Европейский Союз пытается адаптировать законодательное регулирование к технологическим реалиям. В Регламенте отмечается, что «с учетом состояния техники, стоимости реализации и характера, сферы охвата, содержания и целей обработки, а также рисков разной степени вероятности в отношении прав и свобод физических лиц, обусловленных обработкой, контролер обработки данных как на момент определения способов обработки, так и во время обработки принимает надлежащие технические и организационные меры, которые предназначены для реализации принципов защиты персональных данных, такие как сведение к минимуму объема данных и включение необходимых гарантий в процесс обработки в целях выполнения требований Регламента и защиты прав субъектов данных». Этот подход к защите данных активно применяется в области научных исследований, особенно при подаче заявок на получение финансирования, где заявитель должен продемонстрировать надежность системы защиты данных, которая будет внедрена в ходе исследования. Технические аспекты дополняются организационными мерами, которые позволяют обеспечить защиту данных (например, разработка плана управления данными). Регламентом предусмотрено, что «контролер принимает соответствующие технические и организационные меры для обеспечения того, чтобы *по умолчанию* обрабатывались только те персональные данные, которые необходимы для каждой конкретной цели обработки». Указанное требование распространяется на объем собранных персональ-

ных данных, объем их обработки, срок хранения и доступность. Такие меры должны гарантировать невозможность доступа к персональным данным неопределенному числу физических лиц. Предполагается, что сама система обработки должна обеспечивать достаточную степень защиты данных без участия человека. Вместе с тем работа системы не должна быть полностью автономной, поскольку осуществление контроля за сохранностью данных становится практически невозможным.

В дополнение к указанным положениям статьи 9 Регламента вводит общие правила обработки особой категории персональных данных, таких как данные, касающиеся здоровья, или генетические данные. В частности, европейский законодатель отмечает цель обеспечения общественного интереса в качестве правового основания для обработки личных данных конфиденциального характера. При обработке указанного вида данных контролерам необходимо принимать организационные и технические меры, направленные на защиту такого рода информации.

Помимо принципов Регламентом вводятся новые определения и понятия в области защиты персональных данных в сфере научных исследований (данные, касающиеся здоровья, генетическая информация, биометрические данные, анонимные данные, согласие субъекта персональных данных).

НАЗНАЧЕНИЕ СОТРУДНИКА ПО ЗАЩИТЕ ДАННЫХ

Немаловажное значение для организации процесса защиты персональных данных является процедура назначения инспектора по защите персональных данных. В большинстве случаев для исследовательских организаций, для организаций, где сосредоточены базы данных в области здравоохранения, а также в рамках научных проектов назначение такого сотрудника будет обязательным условием осуществления исследовательской деятельности. В соответствии со ст. 37 Регламента, назначение инспектора по защите персональных данных является обязательным, если обработка сведе-

ний осуществляется органом государственной власти или правительственным учреждением, за исключением судов, действующих в рамках своей судебной деятельности; если основным видом деятельности контролера является обработка данных в больших объемах, а также в случае масштабной обработки особой категории данных. Как видим, важным критерием здесь является объем данных, подвергающийся обработке. Стоит отметить, что Регламентом не определено, когда обработка должна рассматриваться в качестве «масштабной». Кроме того, по смыслу Регламента такие виды деятельности, как полное секвенирование генома или использование других высокоэффективных технологий в области здравоохранения, не рассматриваются в качестве предполагающих обработку данных в крупном размере, несмотря на то что в рамках указанных процессов мы имеем дело с большими данными (big data) и особыми рисками в отношении защиты их конфиденциальности.

В тех случаях, когда инспектор по защите персональных данных должен быть назначен в обязательном порядке, его назначение должно производиться с учетом его профессиональных качеств и знаний законодательства и практики в области защиты данных. Такой сотрудник должен обладать достаточными навыками для выполнения своих задач, закрепленных в ст. 39 Регламента. Инспектор по защите персональных данных играет ключевую роль в организациях, поскольку информирует и консультирует контролеров и обработчиков в отношении их обязанностей, контролирует соблюдение требований Регламента, сотрудничает с надзорным органом. В этом смысле контролер данных и обработчик должны надлежащим образом и своевременно консультироваться с инспектором в процессе принятия решений по вопросам защиты данных. Согласно ст. 37(6) Регламента «инспектор по защите данных может быть штатным сотрудником контролера или обработчика или выполнять работу на основе контракта на обслуживание», но в любом случае сотрудник по вопросам защиты данных обязан соблюдать требования конфиденциальности, как это предусмотрено законодательством ЕС

или национальным законодательством. Как указано в ст. 38 Регламента, инспектор по защите персональных данных должен иметь необходимые средства для выполнения своих задач самостоятельно, без получения каких-либо инструкций от контролера или обработчика. Кроме того, контролер или обработчик не имеют права увольнять или налагать санкции на инспектора за выполнение (невыполнение) его задач. Инспектор по защите персональных данных должен непосредственно отчитываться по результатам своей работы перед руководителем контролера или обработчика. Указанные положения Регламента призваны приблизить управление защитой персональных данных к потребностям организаций и сделать защиту персональных данных повседневной практикой.

ПРАВИЛА ИСПОЛЬЗОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИССЛЕДОВАТЕЛЬСКИХ ЦЕЛЯХ

В области научных исследований обработка персональных данных для так называемого вторичного использования (когда цель обработки информации отличается от первоначально поставленной) осуществляется особым образом. Возможность такого способа обработки важна в тех случаях, когда есть необходимость в повторном использовании уже имеющихся персональных данных для целей научного исследования.

Согласно общему принципу, изложенному в ст. 5 Регламента, обработка персональных данных для целей, отличных от тех, для которых персональные данные были первоначально собраны, должна разрешаться только в том случае, если новая цель обработки совместима с целями, для достижения которых персональные данные были первоначально собраны. В данном случае Регламент сохраняет существовавший в рамках Директивы подход, согласно которому «дальнейшая обработка данных для их сохранения и использования в общественных интересах, научно-исследовательских или статистических целях должна рассматриваться как соответствующая закону». Это положение

защищает интересы медицинских центров, научно-исследовательских организаций и биобанков, занимающихся сбором конфиденциальных персональных данных, доступных для использования в исследованиях в будущем. Однако одной совместимости целей исследования в данном случае недостаточно. Контролер обработки персональных данных также должен оценивать целесообразность такой обработки и применение к данным соответствующих мер защиты (выполнение этических стандартов, раздельное хранение данных и т.д.).

В иных случаях повторного использования данных, когда их обработка не основана на однозначном согласии субъекта данных или положениях законодательства ЕС (государства — члена ЕС), контролер должен провести проверку (тест) совместимости целей. Такая проверка (тест) является новым и весьма полезным инструментом, формирующим критерии, которые использует контролер в процессе оценки совместимости целей. В соответствии со ст. 6(4) Регламента «контролер обработки данных определяет наличие связи между целями, для которых персональные данные были первоначально собраны, и целями дальнейшей обработки; условия, в которых персональные данные были собраны, в частности в отношении взаимосвязи между субъектами данных и контролером; характер персональных данных, в частности могут ли подвергаться обработке специальные категории персональных данных или данные о судимости и правонарушениях; возможные последствия вторичной обработки для субъектов данных; наличие соответствующих гарантий, которые могут включать криптографическое закрытие (шифрование) или псевдонимизацию. В тех случаях, когда по результатам проверки (теста) не ставится под сомнение законность и справедливость вторичной обработки персональных данных, тест на совместимость целей считается пройденным и для последующей обработки персональных данных не требуется повторное согласие физического лица. В противном случае такое согласие в соответствии с Регламентом должно быть получено.

УВЕДОМЛЕНИЕ О НАРУШЕНИЯХ В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Основной целью любого законодательного акта, посвященного правовому регулированию защиты персональных данных, является недопущение нарушения конфиденциальности персональных данных или возникновения угрозы такого нарушения. Нарушение в области защиты персональных данных (в том числе в научно-исследовательской деятельности) зачастую определяется как «нарушение безопасности, ведущее к непреднамеренному или умышленному уничтожению, потере, изменению, несанкционированному раскрытию или доступу к персональным данным». Такие нарушения в случае их неустранения (своевременно и надлежащим образом) могут нанести ущерб субъектам данных, в том числе в форме потери контроля над данными или ограничения в правах на них, репутационных рисков, нарушения конфиденциальности.

Регламентом введены более строгие и прозрачные правила относительно уведомления контролера и обработчика. В частности, предусмотрена обязанность контролера и обработчика реагировать быстро и эффективно на любые нарушения (их угрозу) в отношении персональных данных. В случае обнаружения нарушения обработчик должен незамедлительно уведомить об этом контролера обработки данных. Затем информация о нарушении должна быть передана соответствующему надзорному органу и, в определенных случаях, также заинтересованному субъекту данных. Субъект данных незамедлительно информируется контролером о нарушении, в случае если таковое может с высокой вероятностью привести к ущемлению его прав и свобод. Тем не менее, если контролером были предприняты соответствующие технические и организационные меры защиты (например, шифрование данных), индивидуальное информирование субъекта данных заменяется сообщением, доступным широкому

кругу лиц, которое позволяет ознакомиться с фактами и последствиями нарушения. Регламентом предъявляются требования к такому сообщению: оно должно быть ясным и понятным, а также содержать, помимо фактической информации, сведения о том, как действовать в случае обнаружения нарушения в области персональных данных.

Следует обратить внимание на то, что Регламент усиливает ответственность за нарушение правил обработки персональных данных в компаниях — до 20 млн евро (около 1,5 млрд руб.) или 4 % годового общего дохода компании.

НОВЕЛЛЫ, КАСАЮЩИЕСЯ ПРАВ УЧАСТНИКОВ ИССЛЕДОВАНИЯ

В Регламенте закреплены некоторые новые положения относительно прав субъектов данных. Указанные положения касаются хранения персональных данных в общественных интересах, в научных целях, в целях исторического исследования или в статистических целях. Преимущественно эти положения содержатся в ст. 89 Регламента.

Согласие на обработку персональных данных всегда было центральным этическим аспектом участия в исследовательских проектах. Требования Регламента касательно необходимости получения согласия перед каждой обработкой данных (первичной и вторичной), а также возможность использования практики широкого согласия, целью которой является максимальное использование персональных данных, включая особые категории персональных данных, является предметом дискуссий для европейского научного сообщества. Научные круги опасаются, что письменное согласие на обработку персональных данных станет систематическим обязательством². Вместе с тем Регламент определяет письменное согласие как одно из условий (оснований) подтверждения законности обработки данных. Другие условия сформулированы

² См.: *Krzysztofek M.* Post-reform Personal Data Protection in the European Union: General Data Protection Regulation (EU) 2016/679. Wolters Kluwer Law & Business. 2016. P. 23 ; *Lambert P.* Understanding the New European Data Protection Rules CRC Press. 2017. Pp. 151—156.

в ст. 6 и 9 Регламента (касаются персональных данных, не являющихся конфиденциальными, и персональных данных конфиденциального характера). Иные правовые основания, указанные в ст. 6 (для персональных данных) и ст. 9 (для конфиденциальных персональных данных), могут быть использованы для легитимности такой обработки. Здесь важно отметить, что Регламент в этой части не должен вступать в противоречие с другими специализированными законодательными актами ЕС в области научных исследований³, а также с соответствующим национальным законодательством, которое также предусматривает получение согласия на обработку персональных данных. Регламент отмечает, что «обработка специальной категории персональных данных производится в обязательном порядке по соображениям общественного интереса в области здравоохранения без согласия субъекта данных». Такая обработка должна осуществляться при условии принятия надлежащих мер для защиты прав и свобод физических лиц. В этом контексте «здравоохранение» должно определяться в соответствии с Регламентом Европейского парламента и Совета (ЕС) № 1338/2008 — как «все элементы, связанные со здоровьем, а именно состояние здоровья, заболеваемости и инвалидности, факторы, которые оказывают влияние на состояние здоровья, здравоохранения, потребности, ресурсы, выделяемые на здравоохранение, снабжение, и обеспечение всеобщего доступа к медицинской помощи, а также медицинских расходов и финансирования, и причины смертности». Вместе с тем необходимо обратить внимание на то, что обработка данных о здоровье по соображениям общественной безопасности не должна влечь за собой возможность использования обрабатываемой информации в других целях третьими лицами, такими как работодатели или страховые и банковские организации.

Что касается практики использования широкого согласия на обработку персональных данных, то Регламент определяет случаи и условия, когда такое согласие соответствует закону. Регламентом предусматривается возможность субъекта давать согласие на обработку персональных данных в отношении определенных областей научных исследований в соответствии с признанными этическими стандартами. Субъекты могут давать согласие только на определенные области исследований или части исследовательских проектов в той мере, в какой это допускается их целевым назначением. Законность обработки дополняется также условием о том, что согласие субъектов данных может быть сделано для «одной или нескольких конкретных целей».

Субъекты данных имеют комплекс прав, позволяющих им в определенной степени контролировать свои персональную информацию, которая обрабатывается (используется) в ходе исследования. Тем не менее стоит отметить, что уровень гармонизации правового регулирования в области защиты персональных данных в сфере научных исследований на уровне ЕС не высок. Регламентом введены общие принципы обработки персональных данных. Вместе с тем правовое положение субъектов данных в сфере научных исследований практически не затронуто Регламентом. Такая ситуация обусловлена главным образом отсутствием у ЕС полномочий по гармонизации законодательства в области здравоохранения и научных исследований. Союз обладает лишь вспомогательной компетенцией в этих сферах, которые в основном регулируются национальным правом. Таким образом, во исполнение положений Регламента государствам — членам ЕС необходимо предусматривать в своем законодательстве надлежащие гарантии обработки персональных данных для их хранения в общественных и научно-ис-

³ См.: Директива 2004/23 /ЕС Европейского парламента и Совета от 31 марта 2004 года об установлении стандартов качества и безопасности для донорства, закупок, испытаний, обработки, консервации, хранения и распределения тканей и клеток человека; Регламент (ЕУ) 2017/746 Европейского парламента и Совета от 5 апреля 2017 года о медицинских устройствах для диагностики *in vitro* и отмене Директивы 98/79 / ЕС и Решения Комиссии 2010/227 / ЕУ; Директива 2009/41 / ЕС Европейского Парламента и Совета от 6 мая 2009 года по ограниченному использованию генетически модифицированных микроорганизмов.

следовательских целях, а также соблюдения признанных этических стандартов.

ВЫВОД

Знаковым моментом в изменении правового регулирования персональных данных является то, что их защита в различных аспектах теперь осуществляется законодательным актом не в форме *регламента*, а в форме *директивы*. В отличие от регламента, директива ставит перед государствами — членами ЕС только цели. В какой форме и какими методами будет осуществляться достижение этих целей, государства-члены решают самостоятельно. Другая важная черта директив — они могут быть обращены не ко всем государствам-членам, а только к их определенной группе или даже к одному государству — члену ЕС. В отличие от регламентов, директивы не должны быть предельно детализированы. Выбор между регламентом и директивой обуславливается в результате поставленной целью. В отличие от директив, которые являются инструментом гармонизации законодательства государств — членов ЕС, регламенты являются инструментом его унификации. Это означает, что защита персональных данных, в особенности в области научно-исследовательской деятельности, приобретает все большее значение для ЕС и ставится им в приоритет. Поэтому можно говорить о смещении баланса осуществления контрольных функций по их защите от стран-участниц к Европейскому Союзу, который стремится к их концентрации на уровне интеграционной организации в целом. Это подтверждается, в частности, учреждением в рамках ЕС особого наднационального надзор-

ного органа — Европейского совета по защите данных, возглавляемого Европейским инспектором по защите данных, в обязанности которого входит гарантирование единообразного применения настоящего Регламента и издание руководящих указаний, рекомендаций и стандартов передовой практики в соответствующей сфере.

Указанный Регламент призван поддерживать баланс между обеспечением эффективной защиты прав субъектов данных в сетевом обществе и необходимостью обработки (использования) персональных данных, включая данные конфиденциального характера, для научных исследований. Это делает необходимым укрепление и развитие сотрудничества, а также транспарентных отношений между участниками процесса обработки, которые должны принимать активное участие в создании интегрированной системы защиты данных в ЕС. Несмотря на принятие Регламента, содержащего конкретные положения для обеспечения защиты данных при проведении научных исследований, эта сфера отдана на откуп национальному законодателю, в частности в отношении регламентации прав участников исследований. Вместе с тем безусловным преимуществом Регламента является включение в него положений о согласии на обработку данных, о правилах использования персональных данных для цели, отличной от первоначальной, и о системе обработки данных. Кроме того, Регламент впервые отмечает необходимость уважения этических стандартов как важную составляющую требования законности обработки результатов исследований. Несомненно, новеллы, введенные указанным Регламентом, поспособствуют дальнейшему структурированию европейского исследовательского пространства.

БИБЛИОГРАФИЯ

1. *Fuster G. G.* The Emergence of Personal Data Protection as a Fundamental Right of the EU. — Springer Science & Business, 2014. — 274 p.
2. *Gutwirth S., Leenes R., De Hert P., Pouillet Y.* European Data Protection: Coming of Age. — Springer Science & Business Media, 2012. — 440 p.
3. *Krzysztofek M.* Post-reform Personal Data Protection in the European Union: General Data Protection Regulation (EU) 2016/679. — Wolters Kluwer Law & Business, 2016. — 253 p.

4. Lambert P. Understanding the New European Data Protection Rules. — CRC Press, 2017. — 508 p.
5. Lynskey O. The Foundations of EU Data Protection Law. — Oxford University Press, 2015. — 264 p.

Материал поступил в редакцию 6 мая 2019 г.

PERSONAL DATA PROTECTION AND RESEARCH ACTIVITIES: EU LEGAL REGULATION EXPERIENCE ⁴

BARABASHEV Aleksandr Georgievich, PhD in Law, Associate Professor of the Department of Integration and European Law of the Kutafin Moscow State Law University (MSAL)
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

PONOMAREVA Darya Vladimirovna, PhD in Law, Lecturer of the Department of Practical Law of the Kutafin Moscow State Law University (MSAL)
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

Abstract. *Legal regulation of the use of personal data is essential in ensuring the quality of scientific research. Regulation of the European Parliament and of the Council of the European Union No. 2016/679 of April 27, 2016 «On the protection of natural persons with regard to the processing of personal data and on the free movement of such data», repealing Directive 95/46/EC, aims to unify the standards governing the protection of human rights to privacy, certain conditions beyond. This novel, introduced by the Regulation in the EU legal framework, complements and updates the *acquis communautaire* achieved within the framework of Directive 95/46/EC on personal data protection. The Regulation establishes both general rules applicable to any type of personal data processing and special rules applicable to the analysis of certain categories of personal data, such as information obtained during clinical trials. This paper provides an overview of new standards (in force since May 2018) that regulate aspects of personal data processing in the context of research activities (personal health data, genetic, biometric information, etc.)*

Keywords: *European Union, personal data protection, biometric information, genetic information, computer security.*

⁴ The paper is prepared with the financial support of the Russian Foundation for Basic Research, Grant No. 18-29-15022 M «Methods, models and problems of regulation and protection of subjective rights in the field of obtaining, using, disseminating and protecting the results of scientific activity and scientific information.»

СУДЕБНАЯ СИСТЕМА И СУДОУСТРОЙСТВО

В. А. Лаптев*,
Н. И. Соловяненко**

«Судебное облако»: правовые вопросы структурирования и защиты данных¹

Аннотация. Технологии формирования и архитектура облачных баз данных влияют на правовые подходы к обработке и хранению информации в цифровой форме. Обеспечение доступа к данным, хранящимся в «облаке», посредством сети Интернет сделало доступ к информации пользователя экстерриториальным. Современное цифровое общество использует облачные технологии ввиду отсутствия конкурентоспособных альтернатив дистанционного и безопасного хранения данных. При облачном хранении (англ. cloud storage) владелец цифровой информации не осведомлен о конкретном месте нахождения жесткого диска с цифровыми данными. Они хранятся на множестве распределенных в сети серверах. Данные доступны через Интернет в любое время и в любом месте.

В настоящей работе авторы исследуют проблему формирования облачных данных. В качестве конкретного предмета выбрано «судебное облако», используемое в деятельности российских судов. Данный вопрос имеет существенное значение для цифрового государства и бизнеса.

Раскрывается архитектура облачных систем. Приводится характеристика алгоритмов работы облачной системы. Особое внимание уделяется описанию принципов и методов информационной безопасности, в том числе в целях обеспечения интересов государства. Рассмотрены также отдельные аспекты возможного применения искусственного интеллекта при администрировании «судебного облака».

Ключевые слова: информация, облачные хранилища, облачные вычисления, судебное облако, архитектура облака, защита информации, искусственный интеллект.

DOI: 10.17803/1994-1471.2019.103.6.195-204

¹ Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16079 «Цифровая экономика: концептуальные основы правового регулирования бизнеса в России».

© Лаптев В. А., Соловяненко Н. И., 2019

* *Лаптев Василий Андреевич*, кандидат юридических наук, судья Арбитражного суда г. Москвы, доцент кафедры предпринимательского и корпоративного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), старший научный сотрудник сектора предпринимательского и корпоративного права Института государства и права РАН
laptev.va@gmail.com

125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

** *Соловяненко Нина Ивановна*, кандидат юридических наук, старший научный сотрудник сектора предпринимательского и корпоративного права Института государства и права РАН

igpran@igpran.ru

119019, Россия, г. Москва, ул. Знаменка, д. 10

ВВЕДЕНИЕ

Современные цифровые технологии создали почву для нового направления деятельности и, бесспорно, на одном из перспективнейших рынков цифровых услуг — облачные хранилища данных («облака»). В мире IT-технологий широкую популярность получили следующие облачные хранилища: Dropbox, Google Диск, Mega, Яндекс.Диск, OneDrive, Облако Mail.Ru, iCloud, Voh, Nextcloud, SpiderOak, IDrive и pCloud.

Важнейшей задачей государства и отечественной науки в сфере обеспечения информационной безопасности стало стимулирование циркуляции данных «облачных» сервисов внутри страны, о чем свидетельствует Стратегия развития отрасли информационных технологий в Российской Федерации на 2014—2020 годы и на перспективу до 2025 года, утвержденная распоряжением Правительства РФ от 1 ноября 2013 г. № 2036-р². Динамика роста рынка облачных услуг в России отражает востребованность этой цифровой услуги и доверие к ней³. Участниками cloud-рынка выступают как крупнейшие зарубежные компании (например, Huawei и Microsoft), так и российские компании (в частности, МТС). При этом границы государств стираются в цифровом пространстве.

По мнению аналитиков, объем рынка публичных облаков в 2019 г. превысит 200 млрд долл.⁴, первое место займет сектор Software as a Service (SaaS), т.е. программное обеспечение как сервис (служба), второе — Infrastructure as a Service (IaaS), т.е. инфраструктура как сервис, и третье — Platform as a Service (PaaS), т.е. платформа как сервис. Так, Microsoft наглядно показывает типы облачных вычислений (моделей развертывания служб, которые обеспечивают

разный уровень контроля над информацией и разные типы предоставляемых служб)⁵:

- программное обеспечение SaaS позволяет пользователям подключаться к облачным приложениям и использовать их через Интернет (например, электронная почта, ведение календаря и офисные средства);
- платформа PaaS предоставляет пользователям любые приложения: от простых облачных приложений промышленного класса. Включает инфраструктуру (серверы, хранилище и сетевое оборудование), а также ПО промежуточного слоя, средства разработки, бизнес-аналитику (BI), службы системы управления базами данных и др. Услуга PaaS предназначена для поддержки полного жизненного цикла веб-приложения: разработки, тестирования, развертывания, управления и обновления;
- инфраструктура IaaS — это инфраструктура мгновенных вычислений, предоставляемая и управляемая через Интернет. Это один из четырех типов облачных сервисов, наряду с SaaS, PaaS и бессерверным типом⁶.

Технологическая регламентация облачных систем в России определена ГОСТом Р ИСО/МЭК 17826-2015 «Информационные технологии. Интерфейс управления облачными данными (CDMI)»⁷. Так, *облачное хранение (cloud storage)*, или *хранение данных как служба (data storage as a Service — DaaS)*, — «организация сетевых служб виртуализированного хранения и доступа к данным, основанная на требовании заданного уровня службы, что снимает границы масштабируемости; является самообеспечивающимся или не требующим обеспечения и оплачивается в зависимости от потребления» (п. 3.7).

² СЗ РФ. 2013. № 46. Ст. 5955.

³ Карасев С. Российские компании переходят на облачные технологии // URL: <https://servernews.ru/983621> (дата обращения: 01.03.2019).

⁴ URL: <https://servernews.ru/983643> (дата обращения: 01.03.2019).

⁵ URL: <https://azure.microsoft.com/ru-ru/overview/what-is-saas/> (дата обращения: 01.03.2019).

⁶ Бессерверные вычисления — это возможность абстрагирования серверов, инфраструктуры и операционных систем (см.: URL: <https://azure.microsoft.com/ru-ru/overview/serverless-computing/>).

⁷ Приказ Росстандарта от 29 мая 2015 г. № 467-ст.

В ГОСТе 17826-2015 разделяются два вида облаков, иногда именуемые «типами развертывания» (п. 3.21—3.22):

- *частное облако* (private cloud) с предоставлением программы как службы (SaaS), платформы как службы (PaaS), инфраструктуры как службы (IaaS) и (или) хранения данных (DaaS) ограниченному числу пользователей, обычно принадлежащих к одной и той же организации;
- *общественное облако* (public cloud) с предоставлением SaaS, PaaS, IaaS и (или) DaaS потенциально неограниченному количеству пользователей.

На практике дополнительно выделяют третий вид облака — *гибридное облако*, сочетающее в себе элементы частного и общественного облака.

Нередко также разделяются *общественное* и *публичное* облака. Так, *публичное облако* (англ. public cloud) — инфраструктура, предназначенная для свободного использования широкой публикой. Публичное облако может находиться в собственности, управлении и эксплуатации коммерческих, научных и правительственных организаций (или какой-либо их комбинации). Публичное облако физически существует в юрисдикции владельца — поставщика услуг. *Общественное облако* (англ. community cloud) — вид инфраструктуры, предназначенный для использования конкретным сообществом потребителей из организаций, имеющих общие задачи. Общественное облако может находиться в кооперативной (совместной) собственности, управлении и эксплуатации одной или нескольких организаций сообщества или третьей стороны (или какой-либо их комбинации) и может физически существовать как внутри, так и вне юрисдикции владельца.

Весьма удачно преимущества облаков описываются такими ИТ-компаниями, как Microsoft⁸ и КРОК⁹.

В частности, преимущества публичных облаков:

- снижение затрат: нет необходимости приобретать оборудование или программное обеспечение, вы платите только за услугу, которую используете;
- нет обслуживания: ваш поставщик услуг обеспечивает обслуживание;
- почти неограниченная масштабируемость: ресурсы по запросу доступны для удовлетворения потребностей вашего бизнеса;
- высокая надежность: обширная сеть серверов обеспечивает защиту от сбоев.

Преимущества частного облака:

- больше гибкости: ваша организация может настроить свою облачную среду для удовлетворения конкретных потребностей бизнеса;
- улучшенная безопасность: ресурсы не используются совместно с другими, поэтому возможны более высокие уровни контроля и безопасности;

- высокая масштабируемость: частные облака по-прежнему обеспечивают масштабируемость и эффективность публичного облака.

Преимущества гибридных облаков:

- контроль: ваша организация может поддерживать частную инфраструктуру для чувствительных активов;
- гибкость: вы можете использовать дополнительные ресурсы в публичном облаке, когда они вам нужны;
- экономическая эффективность: благодаря возможности масштабирования до общедоступного облака вы платите за дополнительную вычислительную мощность только при необходимости;
- простота: переход к облаку не должен быть слишком сложным, потому что вы можете переходить поэтапно — постепенно увеличивая нагрузку.

Работа облачного хранилища обеспечивается облачными вычислениями (англ. cloud computing), совершаемыми с применением компьютеров и смартфонов при обеспечении сетью Интернет¹⁰, которую можно схематично изобразить следующим образом (рис. 1).

⁸ URL: <https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/>.

⁹ URL: <https://www.croc.ru/solution/ikt-infrastructure/cloud/>.

¹⁰ Подробнее см.: *Vaughan-Nichols S. J. What's the best cloud storage for you?* // URL: <https://www.zdnet.com/article/whats-the-best-cloud-storage-for-you/> (дата обращения: 01.03.2019).



Рис. 1

Таким образом, указанные выше типы облачных вычислений — моделей облачного развертывания данных (частная, публичная, гибридная) — основываются на соответствующих моделях облачных сервисов/служб (SaaS, PaaS, IaaS и бессервисные службы).

В последние годы в отечественном правоведении активно исследуется проблематика работы облачных систем и определяются подходы к их правовому режиму¹¹. Глобализация рынка цифровых услуг отмечается в аналитических материалах Международной корпорации данных — International Data Corporation (IDC)¹².

СТРУКТУРА «СУДЕБНОГО ОБЛАКА» И ПОРЯДОК ФОРМИРОВАНИЯ ДАННЫХ

Архитектура любых облачных систем строится по принципу единства и дифференциации цифровых данных. Авторами настоящей статьи не случайно в качестве предмета исследования выбрано судебное облако (англ. *judicial cloud*). Во-первых, оправление правосудия и эффективная работа российских судов обеспечивают основы конституционного строя Российской Федерации (ст. 123 и 124 Конституции РФ). Во-вторых, технологические решения с учетом тенденций цифровизации во всех областях жизнедеятельности современного общества должны обеспе-

чивать надежность работы облачных данных и защиту информации от третьих лиц.

Оптимизация работы с цифровой информацией является важнейшим вопросом в деятельности государственных органов и частных корпораций во всех странах мира. Так, Верховный суд Соединенного Королевства в своей деятельности столкнулся со следующими проблемами: 1) необходимость предоставления судьям и сотрудникам аппарата суда удаленного доступа к документам вне здания суда; 2) организации должны соответствовать требованиям к отчетности благодаря быстрому и эффективному доступу к информации по ведению дел; 3) рабочая нагрузка судьи возросла на 45 %; 4) технологии должны обеспечивать максимально эффективную работу суда¹³. В качестве решения указанных проблем Верховный суд Соединенного Королевства прибегнул к использованию облачной модели на основе Microsoft Azure, Microsoft Office 365, Microsoft Intune для управления мобильными устройствами и новой системы управления делами на базе Microsoft Dynamics CRM. Таким образом, обеспечена эффективность работы высшего суда и снижены издержки на обработку цифровой информации.

В Китае реформирование судебной системы основывалось в том числе на достижениях быстроразвивающихся технологий и больших данных. Описывая этапы реформирования судебной системы, Alison (Lu) Xu выделяет «информатизацию народных судов 1.0, 2.0 и 3.0», где третья стадия предполагает интеграцию информационно-коммуникационных технологий в повседневную работу судей и применение искусственного интеллекта (AI, *artificial intelligence*) — «интеллектуальный суд». В системе электронного правосудия Китая услуги хранения данных и облачных вычислений поддерживаются, в частности, сервисами Alibaba

¹¹ Например: Карцхия А. А. Облачные технологии: правовой аспект // Российский юридический журнал. 2018. № 6. С. 162—172; Савельев А. И. Правовая природа «облачных» сервисов: свобода договора, авторское право и высокие технологии // Вестник гражданского права. 2015. № 5. С. 62—99; Энтин В. Л. Авторское право в виртуальной реальности (новые возможности и вызовы цифровой эпохи). М., 2017. 216 с.

¹² URL: <https://www.idc.com/>.

¹³ URL: <https://customers.microsoft.com/en-us/story/uks-highest-court-transforms-operations-and-reduces-co>.

Cloud¹⁴. Таким образом, в скором времени китайская судебная система практически полностью перейдет в онлайн-пространство, работающее круглосуточно и вне зависимости от места отправления информации в адрес суда.

В одном из выступлений судья Ronald Forsthoefel отмечал, что суды общей юрисдикции округа Ашленд (штат Огайо, США) полностью основаны на облаке, что позволяет управлять системой управления делами, собирать и обрабатывать документы и даже проводить различные слушания из любой точки мира¹⁵.

Весьма обосновано John C. Eustice исследует вопрос о том, что как только облако выходит за национальные границы (например, при фактическом хранении информации в data-центрах на территории Бразилии, Испании, Аргентины или Уругвая), создается потенциальная опасность, поскольку данные перемещаются в страны или имеют доступ к ним из стран с ограниченным законодательством о конфиденциальности и защите данных¹⁶.

Полагаем, что **принципами построения судебного облака** для российских судов должны выступить:

- свободный доступ резидентам¹⁷ облачного хранилища данных;
- гарантия цифровой защиты информации от третьих лиц;
- резервное копирование (backup copy) данных облака;

- размещение data-центров на территории Российской Федерации;
- наличие альтернативного программного обеспечения для управления облачной инфраструктурой.

Применительно к форме цифровой информации, хранящейся в электронном виде, полагаем возможным размещать в судебном облаке два вида документов¹⁸:

- электронный документ (подписанный электронной подписью);
- скан-образ письменного документа.

Так, в соответствии с п. 1 постановления Пленума Верховного Суда РФ от 26 декабря 2017 г. № 57 «О некоторых вопросах применения законодательства, регулирующего использование документов в электронном виде в деятельности судов общей юрисдикции и арбитражных судов»¹⁹: *электронный образ документа* (электронная копия документа, изготовленного на бумажном носителе) — это переведенная в электронную форму с помощью средств сканирования копия документа, изготовленного на бумажном носителе, заверенная электронной подписью в порядке, установленном законодательством Российской Федерации; *электронный документ* — документ, созданный в электронной форме без предварительного документирования на бумажном носителе, подписанный электронной подписью в порядке, установленном законодательством Российской Федерации.

¹⁴ Alison (Lu) Xu. Chinese judicial justice on the cloud: a future call or a Pandora's box? An analysis of the 'intelligent court system' of China // Information & Communications Technology Law. 2017. 26:1. 59—71. DOI: 10.1080/13600834.2017.1269873.

¹⁵ Анонс конференции «Courts in the Cloud and Tech Talk Dominate Conference», 2019 // URL: http://www.courtnewsOhio.gov/happening/2019/techConf_041819.asp#.XLuGFOszZYi (дата обращения: 19.03.2019).

¹⁶ Eustice J. C. Flying into the cloud without falling: understanding the intersection between data privacy laws and cloud computing solutions // URL: <https://legal.thomsonreuters.com/en/insights/articles/understanding-data-privacy-and-cloud-computing> (дата обращения: 19.03.2019).

¹⁷ Под резидентами понимаются лица, которым предоставлен доступ к документам в электронном виде в судебном облаке.

¹⁸ Подробнее см.: Соловяненко Н. И. Законодательство об электронном документе как фактор актуализации правового пространства для инновационной (цифровой) экономики // Труды ИГП РАН. 2017. Т. 12. № 3. С. 162—175; Электронное правосудие. Электронный документооборот: науч.-практ. пособие / под общ. ред. С. Ю. Чучи; отв. ред. В. А. Лаптев, Н. И. Соловяненко. М.: Проспект, 2017. 240 с.

¹⁹ Бюллетень Верховного Суда РФ. 2018. № 4.

Принимая во внимание положения ГОСТ Р 7.0.8-2013 «Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения»²⁰, электронный архив должен обеспечить аутентичность и достоверность хранящихся в нем электронных документов.

Рациональное комплектование архива и пополнение его новыми электронными документами должно осуществляться с учетом соблюдения соответствующих критериев (времени хранения документов, юридической ценности документов, разновидности конфиденциальной информации в документах и т.д.).

В российских судах в настоящее время применяются *системы автоматизации судопроизводства* — программно-технический комплекс, обеспечивающий ведение судебного делопроизводства, закрепление в электронном виде результатов и хода осуществляемых судом и другими участниками судопроизводства процессуальных действий (в частности, Автоматизированная информационная система Верховного Суда РФ, Государственная автоматизированная система «Правосудие», комплекс автоматизированных информационных систем арбитражных судов, включая автоматизированную информационную систему «Судопроизводство», программный комплекс «Судебно-арбитражное делопроизводство», информационные системы «Мой арбитр», «Картотека арбитражных дел», «Банк решений арбитражных судов»).

Состав электронной информации судебного облака, подлежащей на современном этапе хранению в облаке²¹, по нашему мнению, в зависимости от категории информации должен включать в себя следующее разделы:

1) *судебные акты и иные документы суда*:
— решения;

- определения;
 - постановления;
 - судебные приказы;
 - исполнительные листы;
 - письма, ответы и запросы;
- 2) *архив суда по отдельным категориям дел и журналы учета движения дел*:
— дела, рассматриваемые в порядке упрощенного судопроизводства;
- документы, поступившие в суд в электронном виде;
- аудио- и видеозаписи судебных заседаний;
- журналы учета прохождения жалоб и судебных дел по инстанциям;

3) *заявления и жалобы*:
— иски (заявления);
- апелляционные жалобы;
- кассационные жалобы;
- кассационные и надзорные жалобы в ВС РФ;
- заявления о пересмотре по вновь открывшимся и новым обстоятельствам;

4) *документы по делам*:
— отзыв на иск (заявление);
- встречный иск;
- заявление о вступлении в дело;
- заявления и ходатайства;
- заявления на компенсацию;

5) *банкротство*:
— заявление о признании банкротом;
- заявление о признании физического лица банкротом;
- заявление должника о его банкротстве;
- заявление физического лица о его банкротстве;
- требования кредиторов;
- требования кредиторов к физическому лицу;
- арбитражный управляющий;
- процедуры банкротства;
- иные и произвольные документы.

²⁰ Приказ Росстандарта от 17 октября 2013 г. № 1185-ст.

²¹ При формировании данного перечня документов использовались сведения сайта <https://my.arbitr.ru/#index>, а также Инструкции по делопроизводству в арбитражных судах Российской Федерации (первой, апелляционной и кассационной инстанций), утв. постановлением Пленума Высшего Арбитражного Суда РФ от 25 декабря 2013 г. № 100.

ЗАЩИТА ИНФОРМАЦИИ

Развитие цифровых технологий и переход к хранению информации в электронной форме обеспечиваются надежной защитой цифровой информации и «цифровой гигиеной». Действует важнейший принцип правового регулирования информационных отношений — обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации (ст. 3 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»²²).

Приказом Судебного департамента при Верховном Суде РФ от 2 июня 2017 г. № 96 Инструкция по судебному делопроизводству в верховных судах республик, краевых и областных судах, судах городов федерального значения, судах автономной области и автономных округов была дополнена новой категорией — *ведомственный электронный документооборот*, под которым понимается ведение служебной переписки в электронной форме между судами, Судебным департаментом, органами и учреждениями Судебного департамента по вопросам организационного обеспечения деятельности судов, относящимся непосредственно к компетенции Судебного департамента.

При размещении текстов судебных актов в Интернете суды должны учитывать Положение о порядке размещения текстов судебных актов на официальных сайтах Верховного Суда Российской Федерации, судов общей юрисдикции и арбитражных судов в информационно-телекоммуникационной сети «Интернет»²³. Так, например, в силу п. 3.1 данного Положения тексты судебных актов арбитражных судов, за исключением текстов судебных актов, содержащих сведения государственной или иной охраняемой законом тайны, размещаются на официальных сайтах судов в сети «Интернет» в полном объеме.

Напротив, суды общей юрисдикции, в силу п. 3.3 упомянутого Положения, в целях обеспечения безопасности участников судебного процесса из указанных актов исключают персональные данные:

- а) фамилии, имена и отчества участников судебного процесса;
- б) дата и место рождения, место жительства или пребывания, номера телефонов, реквизиты паспорта или иного документа, удостоверяющего личность;
- в) идентификационные номера налогоплательщиков — физических лиц, индивидуальных предпринимателей, основные государственные регистрационные номера индивидуальных предпринимателей — участников судебного процесса; страховые номера индивидуального лицевого счета;
- г) сведения о месте нахождения земельного участка, здания, сооружения, жилого дома, квартиры, транспортного средства, иные сведения об имуществе и о находящихся в банках или иных кредитных организациях денежных средствах участников судебного процесса, если эти сведения относятся к существу дела.

Вместо исключенных персональных данных используются инициалы, псевдонимы и другие обозначения, не позволяющие идентифицировать участников судебного процесса.

При формировании судебного облака необходимо определить форму и содержание загружаемых в данное облако актов, поскольку его резиденты, имея доступ к данному облаку, могут получить персональные данные.

В данном вопросе эффективным будет применение искусственного интеллекта. Полагая, что ограничения для судей по доступу к какой-либо цифровой информации, в том числе к персональным данным, недопустимы. Судьи во всех случаях не вправе разглашать информацию, полученную при исполнении своих обязанностей (п. 6 ст. 11 Кодекса судейской этики, утвержденного VIII Всероссийским съез-

²² СЗ РФ. 2006. № 31 (1 ч.). Ст. 3448.

²³ Постановление Президиума Верховного Суда РФ от 27 сентября 2017 г.

дом судей 19 декабря 2012 г.²⁴). Исключение могут составлять судебные акты и документы в электронном виде, содержащие сведения государственной тайны, допуск судей к которым устанавливается в особом порядке. При предоставлении доступа к судебному облаку иным резидентам (например, сотрудникам аппарата суда), искусственному интеллекту следует формировать вариативные (по содержанию) электронные виды документов. Например, судьям предоставляется доступ к полному тексту документов в облаке, а сотрудникам аппарата суда — к усеченному, без персональных данных. Такой подход гарантировал бы защиту персональных данных, в том числе от случайного разглашения охраняемых законом сведений.

Значение облачных вычислений в системе цифровой экономики было отмечено в Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы, утвержденной Указом Президента РФ от 9 мая 2017 г. № 203²⁵. Видится существенным вопрос о месте фактического размещения серверов, на которых хранятся данные облака. Полагаем, что единственно верным будет хранение облачных данных на серверах, расположенных исключи-

тельно на территории Российской Федерации. В частности, документы в электронном виде в судебном облаке, содержащие сведения государственной тайны, подпадают под особый правовой режим (ст. 21 и 21.1 Закона РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне»²⁶ и Указ Президента РФ от 30 ноября 1995 г. № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне»²⁷).

ЗАКЛЮЧЕНИЕ

Проведенный анализ позволяет сделать следующие выводы в отношении принципов создания и организации работы «судебного облака»:

1. Создание судебного облака должно основываться на принципах, обеспечивающих информационную безопасность и цифровой суверенитет страны.
2. Местом хранения информации (data-центры) должна быть территория Российской Федерации.
3. Доступ cloud-резидентам к судебному облаку должен иметь дифференцированный подход к соответствующей цифровой информации.

БИБЛИОГРАФИЯ

1. Карасев С. Российские компании переходят на облачные технологии // URL: <https://servernews.ru/983621> (дата обращения: 19.03.2019).
2. Карцхия А. А. Облачные технологии: правовой аспект // Российский юридический журнал. — 2018. — № 6. — С. 162—172.
3. Мухина М. С. Электронное хранение документов в организации // Финансовые и бухгалтерские консультации. — 2016. — № 10. — С. 28—33.
4. Савельев А. И. Правовая природа «облачных» сервисов: свобода договора, авторское право и высокие технологии // Вестник гражданского права. — 2015. — № 5. — С. 62—99.
5. Соловяненко Н. И. Законодательство об электронном документе как фактор актуализации правового пространства для инновационной (цифровой) экономики // Труды ИГП РАН. — 2017. — Т. 12. — № 3. — С. 162—175.
6. Электронное правосудие. Электронный документооборот : научно-практическое пособие / под общ. ред. С. Ю. Чучи ; отв. ред. В. А. Лаптев, Н. И. Соловяненко. — М. : Проспект, 2017. — 240 с.

²⁴ Бюллетень актов по судебной системе. 2013. № 2.

²⁵ СЗ РФ. 2017. № 20. Ст. 2901.

²⁶ СЗ РФ. 1997. № 41. Ст. 8220—8235.

²⁷ СЗ РФ. 1995. № 49. Ст. 4775.

7. Энтин В. Л. Авторское право в виртуальной реальности (новые возможности и вызовы цифровой эпохи). — М., 2017. — 216 с.
8. Alison (Lu) Xu. Chinese judicial justice on the cloud: a future call or a Pandora's box? An analysis of the 'intelligent court system' of China // Information & Communications Technology Law. — 2017. — 26:1. — 59—71. — DOI: 10.1080/13600834.2017.1269873.
9. Eustice J. C. Flying into the cloud without falling: understanding the intersection between data privacy laws and cloud computing solutions // URL: <https://legal.thomsonreuters.com/en/insights/articles/understanding-data-privacy-and-cloud-computing> (дата обращения: 19.03.2019).
10. Lupo G., Bailey J. Designing and Implementing e-Justice Systems: Some Lessons Learned from EU and Canadian Examples // Laws. — 2014. — 3. — 353—387. — DOI: 10.3390/laws3020353.

Материал поступил в редакцию 6 мая 2019 г.

«JUDICIAL CLOUD»: LEGAL ISSUES OF DATA STRUCTURING AND PROTECTION²⁸

LAPTEV Vasiliy Andreevich, PhD in Law, Judge of the Moscow Commercial Court, Associate Professor of the Department of Business and Corporate Law of the Kutafin Moscow State Law University (MSAL), Senior Researcher at the Business and Corporate Law Sector of the Institute of State and Law, Russian Academy of Sciences
laptev.va@gmail.com
125993, Russia, Moscow, ul. Sadovaya-Kudrinskaya, d. 9

SOLOVYANENKO Nina Ivanovna, PhD in Law, Senior Researcher of the Business and Corporate Law Sector of the Institute of State and Law, Russian Academy of Sciences
igpran@igpran.ru
119019, Russia, Moscow, ul. Znamenka, d. 10

Abstract. Formation technologies and cloud database architecture affect legal approaches to the processing and storage of information in digital form. Providing access to data stored in the «cloud» through the Internet made access to user's information extraterritorial. Modern digital society uses cloud technologies due to the lack of competitive alternatives for remote and secure data storage.

In cloud storage, the owner of digital information is not aware of the specific location of the hard disk with digital data. They are stored on multiple servers distributed across the network. Data is available online anytime, anywhere. In this paper, the authors explore the problem of the formation of cloud data. The «judicial cloud» used in the activities of the Russian courts was chosen as a specific subject. This issue is essential for the digital state and business.

The paper discovers the cloud architecture and considers the characteristic of the algorithms of the cloud system. Special attention is given to the description of the principles and methods of information security, including in order to ensure the interests of the state. Some aspects of the possible use of artificial intelligence in the administration of the «judicial cloud» are also considered.

Keywords: information, cloud storage, cloud computing, forensic cloud, cloud architecture, information protection, artificial intelligence.

²⁸ The study is carried out with the financial support of the Russian Foundation for Basic Research, Research project No. 18-29-16079 «Digital Economy: conceptual foundations of legal regulation of business in Russia».

REFERENCES (TRANSLITERATION)

1. Karasev S. Rossijskie kompanii perekhodyat na oblachnye tekhnologii // URL: <https://servernews.ru/983621> (data obrashcheniya: 19.03.2019).
2. Karckhiya A. A. Oblachnye tekhnologii: pravovoj aspekt // Rossijskij yuridicheskij zhurnal. — 2018. — № 6. — S. 162—172.
3. Muhina M. S. Elektronnoe hranenie dokumentov v organizacii // Finansovye i buhgalterskie konsul'tacii. — 2016. — № 10. — S. 28—33.
4. Savel'ev A. I. Pravovaya priroda «oblačnyh» servisov: svoboda dogovora, avtorskoe pravo i vysokie tekhnologii // Vestnik grazhdanskogo prava. — 2015. — № 5. — S. 62—99.
5. Solovyanenko N. I. Zakonodatel'stvo ob elektronnom dokumente kak faktor aktualizacii pravovogo prostranstva dlya innovacionnoj (cifrovoj) ekonomiki // Trudy IGP RAN. — 2017. — T. 12. — № 3. — S. 162—175.
6. Elektronnoe pravosudie. Elektronnyj dokumentooborot : nauchno-prakticheskoe posobie / pod obshch. red. S. Yu. Chuchi ; otv. red. V. A. Laptev, N. I. Solovyanenko. — M. : Prospekt, 2017. — 240 s.
7. Entin V. L. Avtorskoe pravo v virtual'noj real'nosti (novye vozmozhnosti i vyzovy cifrovoj epohi). — M., 2017. — 216 s.

УСЛОВИЯ ОПУБЛИКОВАНИЯ И ТРЕБОВАНИЯ К ПРЕДОСТАВЛЯЕМЫМ В ЖУРНАЛ МАТЕРИАЛАМ И ИХ ОФОРМЛЕНИЮ

Более подробная информация содержится на сайте журнала: arpr.msal.ru

1. В журнале публикуются результаты научных исследований и научные сообщения авторов, изложенные в форме научных статей или рецензий в соответствии с тематикой журнала (далее — статьи).
2. Направление автором статьи для опубликования в журнале считается акцептом, т.е. согласием автора на заключение лицензионного договора о передаче права использования статьи в журнале «Актуальные проблемы российского права».
3. Автор направляет в редакцию журнала статью согласно условиям и порядку предоставления и опубликования статей, а также требованиям к оформлению статей, размещенным на сайте журнала. При несоблюдении указанных требований редакция оставляет за собой право вернуть статью автору без рассмотрения.
4. Требования к содержанию и объему статей:
 - объем статьи должен составлять от 15 до 25 тыс. знаков (с пробелами, с учетом сносок), или 10–15 страниц (формат А4; шрифт Times New Roman, высота шрифта — 14 пунктов; межстрочный интервал — полуторный; абзацный отступ — 1,25 см. Поля: левое — 3 см, правое — 1,5 см, верхнее и нижнее — 2 см). Опубликование материалов меньшего или большего объема должно согласовываться с главным редактором журнала;
 - статья должна быть написана на актуальную тему, должна отвечать критерию новизны, содержать определенное новаторство в подходе к изучаемой теме/проблеме;
 - в статье должны быть отражены результаты научного исследования, основанного на анализе теоретических конструкций, нормативных актов, материалов правоприменительной практики;
 - материал статьи не должен быть только описательным, констатировать существующее положение вещей (статьи, значительная часть которых воспроизводит нормативный материал, будут отклоняться);
 - в материале должна быть соблюдена фактологическая и историческая точность;
 - необходимо обращать внимание на аккуратное использование заимствованного материала, точность цитирования. Ответственность за правильность данных в сносках и пристатейном библиографическом списке несет автор.
5. При оформлении ссылок необходимо руководствоваться библиографическим ГОСТом 7.0.5-2008. В журнале используются подстрочные ссылки, вынесенные из текста вниз страницы (в сноску). Нумерация сплошная (например, с 1-й по 32-ю). Сноски набираются шрифтом Times New Roman, высота шрифта — 12 пунктов, межстрочный интервал — одинарный, абзацный отступ — 1,25. Примеры оформления сносок приводятся на сайте журнала.
6. В библиографический список включается только использованная при написании статьи научная литература. В список не включаются нормативные акты, судебная практика и иные правоприменительные документы или их проекты. Требования к оформлению списка литературы в целом совпадают с требованиями к оформлению ссылок. В списке все работы перечисляются в алфавитном порядке, сначала идут материалы на русском языке, затем — на иностранных языках.

Журнал зарегистрирован Федеральной службой по надзору за соблюдением законодательства
в сфере массовых коммуникаций и охране культурного наследия

ПИ № ФС77-25128 от 7 мая 2014 г.

ISSN 1994-1471

Свободная цена.

Подписка на журнал возможна с любого месяца. Подписной индекс в объединенном каталоге «Пресса России» — 11178.

Вниманию авторов!

*Отдельные материалы журнала размещаются в СПС «КонсультантПлюс» и «ГАРАНТ»,
электронной библиотеке «КиберЛенинка».*

*При использовании опубликованных материалов журнала ссылка
на «Актуальные проблемы российского права» обязательна.*

*Полная или частичная перепечатка материалов допускается только
по письменному разрешению авторов статей или редакции.*

Точка зрения редакции не всегда совпадает с точкой зрения авторов публикаций.

Редактор: *М. В. Баукина*

Компьютерная верстка: *Д. А. Беляков*

Учредитель — Московский государственный юридический университет имени О.Е. Кутафина (МГЮА).

Адрес издателя: 125993, г. Москва, ул. Садовая-Кудринская, д. 9.

Адрес редакции: 125993, г. Москва, ул. Садовая-Кудринская, д. 9.

Тел.: (499) 244-88-88 (доб. 556). E-mail: aprp.msai@yandex.ru

Сайт: aprp.msai.ru

Дата выхода в свет: 30.06.2019. Объем: 23,94 усл.печ.л., формат 60x84/8.

Тираж 150 экз. Печать цифровая. Бумага офсетная.

Отпечатано в Издательском центре Университета имени О.Е. Кутафина (МГЮА).

ВЕСТНИК УНИВЕРСИТЕТА ИМЕНИ О.Е. КУТАФИНА (МГЮА)

- ✓ Свидетельство о регистрации СМИ — ПИ № ФС77-67361 от 5 октября 2016 г., ISSN 2311-5998;
- ✓ издается с 2014 г. — ежемесячно;
- ✓ входит в перечень ВАК России;
- ✓ включен в Российский индекс цитирования (РИНЦ) и Ulrich's Periodicals Directory;
- ✓ каждой статье присваивается индивидуальный международный индекс DOI;
- ✓ отдельные материалы размещаются в СПС «ГАРАНТ» и в электронной библиотеке «КиберЛенинка».

Отличие «Вестника» от журналов, уже издаваемых Университетом (Lex Russica, «Актуальные проблемы российского права»), и от других российских периодических изданий в том, что каждый его выпуск посвящен отдельной отрасли правовых знаний, например трудовому праву и праву социального обеспечения, международному, финансовому праву и т.д.

Журнал знакомит:

- ✓ с основными направлениями развития юридической науки;
- ✓ с актуальными проблемами теории и истории права и государства;
- ✓ конкретных отраслей права; сравнительного правоведения;
- ✓ методики преподавания правовых и общегуманитарных дисциплин, а также иностранных языков в юридическом вузе;
- ✓ с правоприменительной практикой;
- ✓ с путями совершенствования российского законодательства;
- ✓ с известными российскими и зарубежными учеными, их теоретическим наследием;
- ✓ с материалами конференций и круглых столов, проведенных в Университете или с участием профессорско-преподавательского состава Университета в других российских и зарубежных научных центрах;
- ✓ с новой юридической литературой.



KUTAFIN UNIVERSITY LAW REVIEW

Мультиотраслевой научный юридический журнал, который издается на английском языке с сентября 2014 г. и выходит два раза в год. Журнал нацелен на интеграцию российской правовой науки в мировое юридическое сообщество, организацию диалога правоведов по актуальным проблемам теоретической и практической юриспруденции, расширение кругозора и интеллектуальных горизонтов представителей российского правоведения, повышение узнаваемости и авторитета наших ученых-юристов.

Журнал публикует статьи известных и начинающих ученых, юристов-практиков, а также студентов и аспирантов. Главный критерий отбора публикаций — это качество содержания, которое отражает талант автора, его эрудицию и профессионализм в исследуемой сфере, добросовестность и глубину проведенного анализа, использование богатого арсенала научной методологии, актуальность проблематики и новизну результатов проведенного исследования.

Данное издание создает уникальную возможность писать и публиковать научные статьи на английском языке в целях существенного расширения профессиональной читательской аудитории, повышения индекса цитирования, выхода на международный научный уровень.

В качестве авторов, членов редакционного совета и редакционной коллегии с журналом Kutafin University Law Review сотрудничают выдающиеся российские и зарубежные специалисты в различных областях юриспруденции.

The best ideas are always welcomed!



Редакционная подписка на журналы Университета имени О.Е. Кутафина (МГЮА)

Журналы Университета распространяются через объединенный каталог «Пресса России» и интернет-каталог агентства «Книга-Сервис».

Подписаться на журнал можно с любого месяца. Подписные индексы журналов:

«Актуальные проблемы российского права» – 11178, Lex Russica – 11198, «Вестник Университета имени О.Е. Кутафина (МГЮА)» – 40650.

Будем рады видеть Вас в числе подписчиков!

АКТУАЛЬНЫЕ ПРОБЛЕМЫ РОССИЙСКОГО ПРАВА

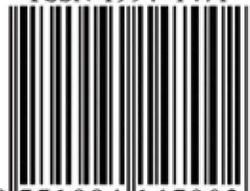
№ 6 (103) ИЮНЬ 2019

Журнал распространяется через
объединенный каталог «Пресса России»
и интернет-каталог агентства «Книга-Сервис».

Подписной индекс: 11178.

Подписаться на журнал можно с любого месяца.

ISSN 1994-1471



9 771994 147002