

ISSN 2221-8351

# КОММЕРЧЕСКОЕ ПРАВО

---

научно-практический журнал

---



№ 3 (Том 42) — 2021

ООО «Издательство «Юрист»  
Москва

**Издательство «ИГ ЮРИСТ»  
Москва**

Учредитель:  
**МГУ им. М.В. Ломоносова**

Главный редактор  
**Пугинский Б.И.**, д.ю.н., профессор

Редакционный совет

**Абросимова Е.А.**, д.ю.н., доцент  
**Амиров А.Т.**, к.ф.н., доцент  
**Андреева Л.В.**, д.ю.н., профессор  
**Бевзенко Р.С.**, к.ю.н., доцент  
**Белов В.А.**, д.ю.н., профессор  
**Олейник О.М.**, д.ю.н., профессор  
**Рассолов И.М.**, д.ю.н., профессор  
**Сидорова Т.Э.**, к.ю.н., доцент  
**Скворцов О.Ю.**, д.ю.н., профессор  
**Турлуковский Я.**, доктор права и философии  
**Цветков И.В.**, д.ю.н., профессор

Ответственный редактор  
**Пальцева М.В.**

**Журнал включен в Российский индекс научного цитирования (РИНЦ)**  
Издание зарегистрировано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).  
Свидетельство о регистрации ПИ № ФС 77–71 195 от 10 октября 2017 г.

**ПОДПИСКА НА ИЗДАНИЕ:**  
Объединенный каталог. Пресса России – 44943  
**Центр редакционной подписки:**  
Тел.: (495) 617-18-88 (многоканальный).

Вниманию авторов!  
Просьба направлять материалы в печатном виде с приложением электронного носителя или по электронной почте. Материалы будущих публикаций принимаются к рассмотрению при наличии информации об авторе и его контактных данных, аннотаций к статье на английском и русском языках, ключевых слов, постраничных сносок, библиографического списка.

Адрес редакции:  
119992, ГСП\_2, Москва, Ленинские горы, д. 1, стр. 13–14,  
IV учебный корпус, Юридический факультет, ауд. 208А  
e-mail: commercial-law@mail.ru

**СПЕЦИАЛЬНЫЙ ВЫПУСК  
«ИНФОРМАЦИОННОЕ ПРАВО»**

<b>Северин В.А.</b> Актуальные направления междисциплинарных исследований правового регулирования и защиты информации .....	4
<b>Чижов И.В., Карасев П.А., Соколов В.В., Шаряпов Р.А., Яценко В.В.</b> Центр проблем информационной безопасности ВМК МГУ: междисциплинарные подходы специалистов для инновационной экономики .....	22
<b>Иващенко Н.П.</b> Роль экономических знаний в подготовке юридических кадров для инновационной экономики .....	36
<b>Варламова А.Н.</b> Регулирование конкурентных отношений в цифровой экономике .....	53
<b>Крылова Н.Е.</b> Криптовалюта: уголовно-правовые аспекты регулирования и охраны .....	64
<b>Борисов М.А.</b> Проблемы доступа к персональным данным в условиях цифровой экономики .....	82
<b>Коржова И.В.</b> Криптоинвесторы из России: миф или реальность .....	96
<b>Калганова М.В.</b> История развития правового регулирования коммерциализации рынка информации в России .....	106
<b>Ильюшина И.С.</b> Истребование персональных данных при приеме на работу .....	118
<b>Робсман Ю.В.</b> Проблемы регулирования инсайдерской информации в законодательстве Российской Федерации .....	131
<b>Северин В.А.</b> Проект сетевой магистерской программы подготовки юристов на межвузовской платформе .....	138
<b>Северин В.А.</b> Магистерская программа «Информационные правоотношения в инновационной экономике» .....	158

**Северин Виталий Андреевич,**

профессор кафедры коммерческого права и основ правоведения  
Юридического факультета Московского государственного университета  
имени М.В. Ломоносова, руководитель магистерской программы  
«Информационные правоотношения в инновационной экономике»,  
доктор юридических наук  
*commercial@law.msu.ru*

## **АКТУАЛЬНЫЕ НАПРАВЛЕНИЯ МЕЖДИСЦИПЛИНАРНЫХ ИССЛЕДОВАНИЙ ПРАВОВОГО РЕГУЛИРОВАНИЯ И ЗАЩИТЫ ИНФОРМАЦИИ**

Цифровизация общественных отношений формирует новую социально-экономическую и правовую реальность, что требует осмысления сущности феномена «информация», внесения изменений в законодательство и корпоративное регулирование, изучения инновационных процессов в целях «перестройки» правовой работы в организациях. Нужны научные данные о состоянии и тенденциях правового регулирования и защиты информации на основе проведения комплексных научных исследований в информационной сфере с участием юристов. Информационное право как наука не получает должного развития в системе российского права вследствие не только недофинансирования, но и отсутствия программы междисциплинарных исследований в информационной сфере и координации усилий творческих коллективов вузовской науки по решению конкретных задач в интересах личности, общества и государства. С учетом опыта читаемых на юридическом факультете МГУ курсов в рамках магистерской программы «Информационные правоотношения в инновационной экономике» в статье анализируются проблемы междисциплинарного характера, недостаточно разработанные в теории информационного права, связанные с гражданским, коммерческим, административным, уголовным и другими отраслями права в цифровой экономике.

Автором сформулирован научный подход и показана актуальность выбора направлений междисциплинарных исследований в области правового регулирования и защиты информации. Содержательно выделены и обоснованы семь направлений, которые могут представлять научный интерес и быть предметом исследований: проблемы правовой работы в организациях высокотехнологического комплекса; понятие и принципы правового регулирования информационных отношений; договоры в сфере обращения информации; коммерциализация прав на результаты интеллектуальной деятельности в организациях; правовые проблемы обеспечения информационной безопасности организаций; принципы и методы правовой защиты информации в интересах личности, общества и государства; разработка концепции междисциплинарного подхода подготовки юристов нового поколения для цифровой экономики.

**Ключевые слова:** цифровая экономика, информационное право, информационная безопасность, правовая работа, междисциплинарные исследования, межкафедретская магистерская программа.

**Vitaly A. Severin**

Professor of the Department of Commercial Law and Fundamentals of Jurisprudence,  
Faculty of Law of the Lomonosov Moscow State University  
Head of the Master's program "Information Legal Relations in the Innovative Economy"  
LL.D.

**CURRENT DIRECTIONS OF INTERDISCIPLINARY RESEARCH  
ON LEGAL REGULATION AND INFORMATION PROTECTION**

Digitalization of public relations forms a new socio-economic and legal reality, which requires understanding the essence of the phenomenon of "information", making changes to legislation and corporate regulation, studying innovative processes in order to "restructure" legal work in organizations. We need scientific data on the state and trends of legal regulation and information protection based on comprehensive scientific research in the information sphere with the participation of lawyers. Information law, as a science, does not receive proper development in the system of Russian law, not only due to underfunding, but also due to the lack of a program of interdisciplinary research in the information sphere and coordination of the efforts of creative teams of university science to solve specific tasks in the interests of the individual, society and the state. Taking into account the experience of the courses taught at the Faculty of Law of Moscow State University within the framework of the master's program "Information Legal Relations in the innovative economy", the article analyzes problems of an interdisciplinary nature that are insufficiently developed in the theory of information law related to civil, commercial, administrative, criminal and other branches of law in the digital economy.

The author formulates a scientific approach and shows the relevance of choosing the directions of interdisciplinary research in the field of legal regulation and information protection. Seven directions that can be of scientific interest and be the subject of research are meaningfully identified and justified: problems of legal work in organizations of a high-tech complex; the concept and principles of legal regulation of information relations; contracts in the field of information circulation; commercialization of rights to the results of intellectual activity in organizations; legal problems of ensuring information security of organizations; principles and methods of legal protection of information in the interests of the individual, society and the state; development of the concept of an interdisciplinary approach to training a new generation of lawyers for the digital economy.

**Keywords:** digital economy, information law, information security, legal work, interdisciplinary research, inter-faculty master's program.

В России с 2017 года действует полномасштабная программа «Цифровая экономика Российской Федерации»<sup>1</sup>, которая ориентирует отрасли на переход от функционирования обычных рынков и системы управления

<sup>1</sup> См.: Программа «Цифровая экономика Российской Федерации»: утв. Распоряжением Правительства РФ от 28 июля 2017 г. № 1632-Р «Система управления реализацией программы «Цифровая экономика Российской Федерации» // URL: <https://itforum.admhmao.ru/upload/iblock/4ae/05-a.sidorov-rostelekom.pdf>

к инновационному механизму с проникновением информации и цифровых технологий во все сферы хозяйственной деятельности. Процесс цифровизации затрагивает регулирование сферы производства, финансового обращения и электронной торговли, где для коммуникации используется среда сети Интернет<sup>2</sup>. В состав национальной программы входят федеральные проекты «Нормативное регулирование цифровой среды», «Кадры для цифровой экономики», «Информационная инфраструктура», «Информационная безопасность», «Цифровые технологии», «Цифровое государственное управление», «Искусственный интеллект»<sup>3</sup>. В разработке названных проектов принимают участие и юристы, главной задачей которых является подготовка на основе анализа «классических» правовых конструкций предложений по принятию систематизированных правовых норм и требований к механизмам цифровой экономики, основанном на гибком подходе в каждой сфере, что позволит разграничить правовое и техническое регулирование, избежать ведомственного подхода и фрагментарности регулирования. Для решения этой задачи должен быть разработан единый понятийный аппарат в сфере правового обеспечения инновационной (цифровой) экономики. Отсутствие соответствующей нормативной правовой базы в отношении изменения правовых режимов регулирования ИТ технологий, сохранности информации, которая затрагивает в новых условиях интересы различных субъектов права, обуславливает необходимость проведения научно-исследовательских работ на междисциплинарной основе.

Министерством науки и высшего образования РФ от 24 февраля 2021 г. была утверждена новая номенклатура научных специальностей, по которым присуждаются ученые степени (далее — номенклатура)<sup>4</sup>. Юридические науки были включены в раздел 5 «Социальные и гуманитарные науки» в виде пяти блоков: 5.1.1. Теоретико-исторические правовые науки; 5.1.2. Публично-правовые (государственно-правовые) науки; 5.1.3. Частноправовые (цивилистические) науки; 5.1.4. Уголовно-правовые науки; 5.1.5. Международно-правовые науки. В прежней номенклатуре груп-

<sup>2</sup> См.: Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_216363/](http://www.consultant.ru/document/cons_doc_LAW_216363/)

<sup>3</sup> См.: Цифровая экономика РФ // Сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: <https://digital.gov.ru/ru/activity/directions/858/>

<sup>4</sup> См.: Приказ Министерства науки и высшего образования РФ от 24 февраля 2021 г. № 118 «Об утверждении номенклатуры научных специальностей, по которым присуждаются ученые степени, и внесении изменения в Положение о совете по защите диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук, утвержденное приказом Министерства образования и науки Российской Федерации от 10 ноября 2017 г. № 1093». URL: <https://www.garant.ru/products/ipo/prime/doc/400450248/>

па «Юриспруденция» включала в себя 15 специальностей<sup>5</sup>, в том числе «Информационное право» — 12.00.13. По мнению специалистов, в новой номенклатуре эта специальность, вероятно, будет включена в блок «Публично-правовые (государственно-правовые) науки»<sup>6</sup>. Такой подход, по нашему мнению, объясняется тем, что ранее специальность 12.00.14 — «Административное право, финансовое право и информационное право» включала «Информационное право», что подчеркивает его тесную связь с административным правом. Однако с принятием Кодекса административного судопроизводства РФ<sup>7</sup> паспорт специальности 12.00.14 — «Административное право, финансовое право и информационное право» был изменен Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации (далее — ВАК). До принятия действующей сегодня номенклатуры специальность 12.00.14 включала «Административное право; административный процесс». Отдельно были выделены специальности «Финансовое право» (12.00.07) и «Информационное право» (12.00.13). В соответствии с письмом ВАК<sup>8</sup> решение вопроса о включении информационного права в тот или иной блок юридической науки следует ожидать не ранее середины следующего года.

Выборочный анализ кандидатских и докторских диссертаций, защищенных за последние 20 лет<sup>9</sup>, показывает, что многие исследования по информационному праву тесно связаны с использованием понятийного аппарата не только базовых отраслей конституционного, гражданского, административного и уголовного права, но и других областей науки, в частности экономики, техники и технологий, информатики,

<sup>5</sup> См.: Приказ Министерства образования и науки РФ от 23 октября 2017 г. № 1027 «Об утверждении номенклатуры научных специальностей, по которым присуждаются ученые степени». URL: <https://www.garant.ru/products/ipo/prime/doc/71714408/>

<sup>6</sup> См.: Муранов А. Юрнауки в проекте Номенклатуры научных специальностей // URL: [https://zakon.ru/blog/2020/10/08/yurnauki\\_v\\_proekte\\_nomenklatury\\_nauchnyh\\_sposobnostej\\_vazhna\\_dlya\\_zaschity\\_dissertacij\\_zerkalo\\_sovr](https://zakon.ru/blog/2020/10/08/yurnauki_v_proekte_nomenklatury_nauchnyh_sposobnostej_vazhna_dlya_zaschity_dissertacij_zerkalo_sovr)

<sup>7</sup> См.: Кодекс административного судопроизводства Российской Федерации от 8 марта 2015 г. № 21-ФЗ (ред. от 30.04.2021, с изм. от 15.07.2021) // URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_176147/](http://www.consultant.ru/document/cons_doc_LAW_176147/)

<sup>8</sup> См.: Письмо ВАК Минобрнауки России от 13 мая 2021 г. № 382-02 «О применении новой номенклатуры научных специальностей». URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_384592/](http://www.consultant.ru/document/cons_doc_LAW_384592/)

<sup>9</sup> См.: Бычкова А.М. Информационное право: статистическое исследование тематики и количества диссертационных работ по научной специальности 12.00.13 // Пролог: журнал о праве. 2020. № 4 (28). URL: <https://cyberleninka.ru/article/n/informatsionnoe-pravo-statisticheskoe-issledovanie-tematiki-i-kolichestva-dissertatsionnyh-rabot-po-nauchnoy-sposobnosti-12-00-13> (дата обращения: 27.08.2021); Темы диссертаций и авторефератов по специальности ВАК РФ 12.00.14 «Административное право, финансовое право, информационное право» // Электронная библиотека диссертаций. URL: <https://www.disserscat.com/catalog/yuridicheskie-nauki/administrativnoe-pravo-finansovoe-pravo-informatsionnoe-pravo?page=120>

вычислительной техники и управления, что подчеркивает их междисциплинарный характер.

В условиях цифровизации распространенность нарушений информационной безопасности предприятий и организаций, общественный резонанс от установленных на них режимных ограничений, от возможной утечки охраняемой информации связаны с причинением не только материального ущерба хозяйствующим субъектам, но и существенного вреда, причиняемого личным, общественным и государственным интересам. Поэтому независимо от включения информационного права в тот или иной блок «Юридические науки» сохранится тенденция его связи с базовыми отраслями права, поскольку в информационной среде имеются проблемы уголовно-правового, криминологического, административно-правового и гражданско-правового характера, связанные с содержанием понятия «информация» на основе философского осмысления феномена информации<sup>10</sup>.

*В числе проблем уголовно-правового и криминологического характера* приоритетным является исследование характеристики правонарушений норм законов и подзаконных актов, договоров, регулирующих отношения в цифровой экономике, представляющей собой определенную систему признаков, использование которых необходимо для предупреждения разглашения (утечки) ценных сведений в информационной среде. В различных секторах инновационной экономики, имеющих свои структурные, технологические и иные особенности, могут быть отдельные исследования для получения оценки степени актуальности борьбы с такими правонарушениями в целях достижения оптимального результата использования сил и средств профилактического воздействия.

Монополистом информации, составляющей государственную тайну, является государство. При владении, пользовании и распоряжении такой информацией полномочные государственные органы вступают в имущественные и обязательственные отношения с другими субъектами гражданского права. В частности, не решена проблема компенсации затрат частных лиц при передаче информационных ресурсов в связи с требованиями государства по их засекречиванию. Возникают ли при этом договорные отношения, а в случаях неправомерных действий государственных органов также встают вопросы о возмещении ущерба, причиненного

<sup>10</sup> См.: Богатырева Е.Н. Феномен информации в контексте научного познания: философский анализ: дис. ... канд. философ. наук, 2000 // Научная электронная библиотека диссертаций и авторефератов disserCat. URL: <https://www.dissercat.com/content/fenomen-informatsii-v-kontekste-nauchnogo-poznaniya-filosofskii-analiz> ; Кадочников В.П. Философские проблемы научных исследований феномена информации // ОНВ. 2007. № 2 (54). URL: <https://cyberleninka.ru/article/n/filosofskie-problemy-nauchnyh-issledovaniy-fenomenu-informatsii> (дата обращения: 05.09.2021), и др.



гражданам либо организациям. Нуждаются в анализе договорные отношения, которые возникают между юридическими лицами и государственными органами в процессе передачи сведений, документов либо опытных образцов, составляющих государственную тайну, при выполнении научно-исследовательских и опытно-конструкторских работ. Отдельного изучения заслуживает проблема передачи сведений, содержащих государственную тайну, оборонными предприятиями, когда по решению Правительства РФ на основании контракта иностранным государствам передается сопроводительная техническая и другая документация к специальным изделиям (военная техника и вооружение). В данном случае нарушение режима секретности сведений, составляющих предмет контракта, другой стороной может причинить существенный вред интересам нашего государства.

Проблемы *административно-правового характера* касаются разработки и принятия федерального закона о служебной тайне, обоснование на его основе содержания и объема сведений, составляющих служебную тайну, определение порядка допуска и доступа лиц к таким сведениям и прозрачность мер по их защите государственными и муниципальными органами управления. В правовом плане важным является определение понятия информации, составляющей служебную тайну, и ограничение ее от государственной тайны. В советский период служебная тайна являлась своеобразным «шлейфом» государственной тайны, продолжением последней с меньшей степенью секретности, причем в ряде нормативных правовых актов указывалось на возможность ведомств иметь такую тайну. В настоящее время отношения по поводу обращения «служебной тайны» регулируются ведомственными нормативными правовыми актами, механизм в отличие от государственной и коммерческой тайны законодательно не закреплен. Такое положение дел может быть связано с необоснованным засекречиванием информации и причинением ущерба общественным, корпоративным и личным интересам, либо способствовать открытию возможных каналов утечки важной для государства информации.

Проблемы *гражданско-правового характера* в сфере обращения информации в основном касаются правового понимания в гражданском обороте информации как ценного продукта наряду с предметами материального мира. Использование в предпринимательской (коммерческой) деятельности коммерчески значимой информации, защищаемой нормами комплексного правового института коммерческой тайны, требует в условиях цифровизации иного подхода к прежнему порядку допуска и доступа лиц к информации и к мерам правовой охраны ее конфиденциальности. Представляется важным исследование новых форм взаимодействия субъектов гражданского права в сфере цифрового обращения и разработка методики определения ущерба, причиняемого вследствие разгла-

шения (утечки) охраняемой информации посредством неправомерного (халатного) использования информационно-коммуникационных технологий.

Опыт автора по научному руководству дипломными работами (специалистов, бакалавров, магистров) и реализация магистерской программы «Информационные правоотношения в инновационной экономике», открытой на кафедре коммерческого права и основ правоведения, свидетельствуют, что студенты чаще всего обращаются к исследованию проблем, которые обозначены в программных документах инновационного развития общества и государства как приоритетные в условиях цифровизации. Так, за последние два десятилетия студентами в рамках дипломных работ были выполнены исследования по следующим темам (указаны по убывающей в годах): «Договоры в инновационной деятельности в условиях цифровизации экономики», «Правовое регулирование и защита коммерческих секретов в Китайской Народной Республике», «Договорное регулирование отношений в информационной сфере Китая», «Правовые вопросы применения смарт-договоров в торговом обороте», «Правовое регулирование криптовалюты в условиях цифровой экономики», «Механизмы правовой защиты информации в инновационной экономике», «Цифровые продукты как объект гражданского (коммерческого) права», «Сравнительное исследование передачи прав на единые технологии по законодательству России и ЕС», «Служебная тайна: регулирование и защита», «Регулирование правоотношений в области искусственного интеллекта», «Правовое регулирование технологии распределенного реестра (блокчейн)», «Правовое регулирование и защита персональных данных в организациях», «Регулирование и защита информации при использовании облачных технологий», «Правовое регулирование коммерциализации научных исследований в инновационной экономике России», «Правовое регулирование информации в гражданском обороте в условиях цифровой экономики», «Правовое регулирование защиты персональных данных пользователей интернет-ресурсов», «Правовое обеспечение инновационной деятельности и коммерциализации научных разработок в организации», «Защита интеллектуальной собственности в условиях развития информационных технологий», «Правовая работа в коммерческой организации», «Правовые вопросы информационного обеспечения торговой деятельности», «Правовое регулирование информационных отношений на этапах выполнения НИОКР», «Договоры на оказание информационных и дизайнерских услуг в современном европейском частном праве», «Правовая защита информационных ресурсов коммерческой организации», «Формирование и защита деловой репутации коммерческой организации», «Обеспечение коммерческой тайны в торговом обороте» и др.

Анализ тематики дипломных работ, выводов и предложений по разработке теоретических положений, совершенствования законодательства и практики его исполнения в информационной сфере позволяет выделить следующие актуальные направления междисциплинарных исследований: 1) проблемы правовой работы в организациях высокотехнологичного комплекса; 2) понятие и принципы правового регулирования информационных отношений; 3) договоры в сфере обращения информации; 4) коммерциализация прав на результаты интеллектуальной деятельности в организациях; 5) правовые проблемы обеспечения информационной безопасности организаций; 6) принципы и методы правовой защиты информации в интересах личности, общества и государства; 7) разработка концепции междисциплинарного подхода подготовки юристов нового поколения для цифровой экономики. Кратко рассмотрим содержание названных направлений.

**Проблемы правовой работы в организациях высокотехнологичного комплекса.** Программой «Цифровая экономика Российской Федерации»<sup>11</sup> определены новые задачи по правовому обеспечению деятельности вновь создаваемых высокотехнологичных комплексов (организаций). Традиционный подход к пониманию правовой работы здесь уже не работает, нужны новые разработки понятийного аппарата. Цифровая реальность требует от юристов перестройки в плане повышения уровня знаний об инновационных процессах, происходящих в обществе и государстве. Этого можно достичь путем изучения социально-экономических причин, сдерживающих инновационное развитие России. Именно эти причины обуславливают проблемы правового обеспечения цифровой экономики на уровне общества, государства и отдельной организации. Перестройка должна коснуться определения приоритетных направлений деятельности юридической службы в условиях информационного общества. Особо это касается изменения механизмов договорной работы, когда происходит использование информационных технологий при заключении сделки и выполнении договорных обязательств. С учетом специфики правового обеспечения научно-исследовательских и опытно-конструкторских работ, а также процессов коммерциализации прав на результаты интеллектуальной деятельности эти направления правовой работы требуют разработки руководящих документов для юристов в виде регламента и методики.

**Понятие и принципы правового регулирования информационных отношений.** Исследование правоведами понятийного аппарата понимания и правового регулирования оборота информации должно базироваться

<sup>11</sup> См.: Программа «Цифровая экономика Российской Федерации»: утв. распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р. URL: <http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf>

на методологии, предложенной В.Н. Лопатиным<sup>12</sup>, который предлагает исходить при объяснении феномена «информация» из анализа соотношения категорий «информация и материя», «информация и человек», «информация и электронное государство», и считает, что «... (информация и материя) — двуединая первооснова существующего мира»<sup>13</sup>. Инновационный процесс в деятельности организаций связан с реализацией результатов интеллектуальной деятельности и использованием коммерчески значимой информации<sup>14</sup>. Юристам важно понимание категории «инновационная деятельность», которая достаточно изучена в экономической науке, тогда как юристы делают лишь первые шаги в изучении механизмов регулирования инновационных отношений в организациях. Такое состояние можно объяснить медленным развитием законодательства, отсутствие результатов научных исследований в данной области, когда, по существу, размыт предмет правового регулирования инновационной деятельности, что справедливо отмечают ученые-правоведы<sup>15</sup>. На наш взгляд, при изучении общественных отношений, составляющих предмет инновационного права, следует обратить внимание на структурные элементы правового регулирования отношений, связанных с созданием новшеств в процессе выполнения НИОКР; с государственным воздействием на инновационную деятельность административного характера; с процессами коммерциализации, начиная от запуска в производство и выхода на рынок информационного продукта; с улучшением правовой охраны результатов интеллектуальной деятельности и защиты информации. Учитывая происходящие процессы саморегулирования в отдельных отраслях экономики, в том числе в информационной сфере, важным представляется определение путей формирования саморегулируемых организаций в данной сфере и разработка методики для практического использования.

**Договоры в сфере обращения информации.** В условиях информационного общества для нашей страны важной задачей является формирование информационной среды, доступных информационных ресурсов (продуктов, услуг), предназначенных для удовлетворения информационных потребностей личности, общества и государства. Информация овеществляется во всех фазах общественного производства и составляет «нулевой» цикл по отношению к любому производимому товару, выполняемой ра-

<sup>12</sup> См.: Лопатин В.Н. Методологические проблемы понимания и правового регулирования оборота информации. В кн.: Северин В.А. Актуальные вопросы правового регулирования и защиты информации в России (избранные труды). М., 2021. С. 15–21.

<sup>13</sup> См.: Лопатин В.Н. Информационное право : учебник для вузов. 3-е изд., с изм. и доп. М. : Проспект, 2021. С. 656.

<sup>14</sup> См.: Северин В.А. Коммерческая тайна в России. 2-е изд. М. : Зерцало-М, 2009. С. 38–57.

<sup>15</sup> См.: Инновационное право : учебник / А.И. Маркеев, В.А. Свиридов, Н.М. Тюкавкин, Р.З. Юсупов / отв. ред. доктор юридических наук, профессор А.В. Юдин. Самара : Издательство Самарского университета, 2020. С. 46–58, и др.

боте и оказываемой услуге. Юристы чаще всего имеют дело с «документированной информацией», зафиксированной на материальном бумажном или электронном носителе с реквизитами, позволяющими ее идентифицировать. Поэтому «овеществление информации» происходит путем закрепления ее на материальном носителе. Цифровизация вносит изменения в привычные акты купли-продажи товаров (продавец, покупатель, посредник). Потребители информации чаще всего в электронном виде, заключают с соответствующими субъектами, владеющими информацией, договоры о возмездном оказании информационных услуг, связанных с поиском необходимой информации, ее обработкой и хранением. На практике интерес представляют договоры о пользовании автоматизированными информационными системами, банками данных, компьютерными сетями. Заключение таких договоров обусловлено условиями конфиденциальности передачи и использования информации (формы, способы, ответственность). В условиях конкуренции получение прибыли организацией и ее выживаемость на рынке зависит от получения и умения сохранить коммерчески значимую информацию, неизвестную конкурентам, а также от способности правильно распорядиться ею на рынке. Речь идет о коммерческой тайне информации, возникающей в процессе производства и обмена товаров (работ, услуг). Следует отметить, что исследователи еще недостаточно уделяют внимание изучению форм проявления коммерческой тайны в производственных процессах, где используются информационные технологии и искусственный интеллект (обеспечивающие, обслуживающие, вспомогательные и основные процессы), согласно принятой в экономической науке классификации.

Особое внимание к охране конфиденциальности информации стороны должны уделить в период, предшествующий заключению договора. Преддоговорные контакты лучше осуществлять после согласования сторонами положения об обеспечении конфиденциальности информации, которое затем будет неотъемлемой частью заключенного договора. Закон не обязывает заключение такого договора, его условия выработаны практикой. На этапе заключения договоров стороны вырабатывают условия, определяющие порядок обеспечения конфиденциальности информации при выполнении совместных работ (НИОКР, маркетинговых исследований); при передаче информационных продуктов («ноу-хау», информации, содержащейся в базе данных и др.); при оказании возмездных информационных услуг (консультационное и техническое содействие, юридический консалтинг и др.). Содержание и формулировки этих условий требуют проведения исследования.

**Коммерциализация прав на результаты интеллектуальной деятельности в организациях.** Коммерциализация, являясь элементом национальной инновационной системы России, означает процесс перевода результатов

научных исследований, полученных в виде новой технической и технологической информации в сферу производства новых продуктов, услуг в целях получения прибыли и иной коммерческой выгоды.

Коммерциализация как процесс представляет собой ряд сложных и взаимосвязанных этапов по подготовке инновационного предложения, экспертизе технологии инвесторами, привлечению инвестиций, договорному закреплению отношений между всеми участниками процесса, распределению прав на будущую интеллектуальную собственность, освоению результатов в производстве, сопровождению инновационного продукта и его дальнейшей модификации, которые требуют правового обеспечения. Эти процессы должны быть осмыслены юристами, к ним нужно подходить системно, имея в виду состояние законодательной базы, практики регулирования корпоративных и договорных отношений, а также использования различных способов защиты информации.

Для практической деятельности юриста важно наличие методики, в которой содержатся положения по выбору форм и методов правового обеспечения коммерциализации результатов научных исследований. Отсутствие единой концепции в рассматриваемой сфере обуславливает недостатки действующего законодательства и необходимость его совершенствования. Анализ положений о юридических департаментах показывает, что в условиях цифровой экономики компетенции юридических служб для правового обеспечения научно-технической и инновационной деятельности явно недостаточно. Нужен анализ причин, которые препятствуют процессам коммерциализации на уровне организаций с целью выработки концепции регулирования правоотношений в этой сфере с участием юристов. К этому нужно добавить недостатки в подготовке юридических кадров, способных грамотно обеспечивать этапы коммерциализации, что подтверждает необходимость внесения изменений в учебные программы.

**Правовые проблемы обеспечения информационной безопасности организаций.** Информационную безопасность организации можно определить как состояние защищенности ее интересов в информационной среде от внутренних и внешних источников угроз, последствиями которых может быть причинение ей материального и иного ущерба, что многократно возрастает в условиях цифровизации. Однако методик, позволяющих определить размер ущерба государственных и частных субъектов хозяйственной деятельности в информационной сфере, не существует. Представляется, что, отталкиваясь от решения этой задачи, следует выделить узловые проблемы исследования: характеристика элементов информационной безопасности организации; анализ определяющего влияния экономических процессов цифровизации, связанных с регулированием информационных отношений; обоснование правовых режимов допуска и

доступа к информации в организации; рассмотрение предупреждения нарушений средствами правового, организационного и технического воздействия в сфере обращения охраняемой информации как главного направления обеспечения информационной безопасности организации; изучение проявления нарушений режима секретности (конфиденциальности) на различных каналах утечки информации, анализ характеристики личности нарушителей режима секретности и классификация причин и обстоятельств, способствующих совершению нарушений режима секретности; анализ организационных основ контроля в этой сфере и защиты прав на охраняемую информацию в судебном порядке. Это неполный перечень проблем, которые должны быть предметом внимания исследователей. Причем целью исследования должно быть изучение правовых проблем информационной безопасности не только применительно к отдельным организационно-правовым формам организаций или в зависимости от их отраслевой структуры, но и в целом как единого комплекса вопросов, отражающих общий подход к правовому регулированию, обеспечению информационной безопасности организации и защиты ее права на информацию.

**Принципы и методы правовой защиты информации в интересах личности, общества и государства.** В числе охраняемой на основе федеральных законов информации следует выделить такие ее виды, как государственно значимая информация (государственная и служебная тайны) для обеспечения обороноспособности и безопасности российского государства, коммерчески значимая информация (коммерческая тайна), используемая организациями для обеспечения своей безопасности с целью получения максимальной прибыли, лично значимая информация (персональные данные) для защиты интересов частной жизни личности (граждан). В условиях информационного общества и цифровой экономики названные правовые институты, которые возникли в нашей стране в разное время и продолжают функционировать, нуждаются в разной глубине анализа форм и методов с учетом применяемых информационных технологий, искусственного интеллекта. Нужно отметить, что в условиях рыночной экономики исследователи чаще всего обращаются к коммерческой тайне как институту, существовавшему в дореволюционной капиталистической России. Автором настоящей статьи разработана научная концепция гражданско-правового регулирования информации и охраны ее конфиденциальности<sup>16</sup>, но цифровизация экономики вносит изменения в гражданский оборот информации, поэтому нужны исследования новых форм и методов сбора, хранения, передачи и защиты информации внутри организации и в договорных отношениях.

<sup>16</sup> См.: Северин В.А. Коммерческая тайна в России : монография. М. : Зерцало-М, 2007. 614 с.

Проблемы защиты сведений, составляющих государственную тайну в новой демократической России, засекречивания и рассекречивания информации, личности нарушителей режима секретности, причин и обстоятельств, способствующих таким нарушениям, и меры предупреждения не получили за последние 30 лет должного рассмотрения в научной литературе. Отсутствуют четкие критерии оценки ущерба, причиняемого обороноспособности и безопасности государства при разглашении (передачи) сведений, составляющих государственную тайну, практически не изучаются формы воспитательно-предупредительной работы в трудовых коллективах в новых условиях, порой принимаемые меры уголовной ответственности не соответствуют степени общественной опасности данного преступления.

Наряду с правовым институтом государственной тайны в нашей стране функционирует институт служебной тайны, который регулирует деятельность государственных органов и органов местного самоуправления по поводу сбора, получения, передачи и защиты служебной информации. Федерального закона в этой сфере нет, используется гриф «Для служебного пользования» и др., но все это на подзаконном уровне регулирования. Проблема состоит в том, что с принятием Закона «О государственной тайне» сведения с грифом «Секретно» были отнесены к государственной тайне. Понятие «служебная тайна» утратило прежнее содержание по степени секретности сведений, и к этому понятию не может применяться гриф «Секретно». Речь идет о необходимости концептуального изложения сущности служебной тайны, разработки предложений по внесению изменения в законодательство или принятия нового Федерального закона о служебной тайне, и на этой основе обоснование методики, необходимой для работы служб безопасности. Имеются проблемы правового регулирования и защиты инсайдерской информации в бизнесе, незаконное использование такой информации причиняет значительный вред организациям, однако исследования в данной сфере практически не ведутся.

Правовой институт персональных данных начал формироваться относительно недавно. В этой области нужна разработка методики, на основе которой администрация принимает решение о готовности работы с персональными данными и интенсивности применения внутрикорпоративных сил и средств. Содержанием методики должны быть предложены на концептуальном уровне комплексные меры организационно-правового и технического характера для обеспечения безопасности оборота персональных данных в условиях цифровизации организаций.

**Разработка концепции междисциплинарного подхода подготовки юристов нового поколения для цифровой экономики.** Актуальность подготовки юристов для цифровой экономики является важной задачей государства. В новых условиях юристы недостаточно подготовлены к право-



вому обеспечению инновационной деятельности, недостаточно владеют способами коммерциализации результатов научных разработок и защиты информации. На Юридическом факультете МГУ в 2016 г. была открыта новая магистерская программа «Информационные правоотношения в инновационной экономике», которая по существу является межфакультетской программой МГУ. Учебные курсы читают преподаватели Юридического факультета, Высшей школы государственного аудита, Экономического факультета, Факультета вычислительной математики и кибернетики, Военного учебного центра при МГУ и Института проблем информационной безопасности МГУ. Данная программа отличается от других магистерских программ, открытых в Московском университете и других вузах. В 2018 г. состоялся первый выпуск магистров по данной программе.

Анализ внедрения магистерской программы показывает, что для всестороннего понимания и сопровождения процесса превращения идеи в инновационный продукт нужны не только юридические, но и экономические и технические знания, которые позволят представить взаимосвязанные этапы научно-технической и инновационной деятельности. Обращение к проблемам информационного, гражданского и коммерческого права, а также дисциплин публично-правового характера не позволяет в полной мере подготовить магистров для работы в области интеллектуальных прав и защиты информации. Нужен комплексный подход подготовки магистров на основе междисциплинарных знаний в области регулирования информационных правоотношений, экономики информационных ресурсов, систем и технологии и информационного менеджмента. Возможно, при сбалансированном подходе к структуре учебных курсов по праву, экономике и другим наукам следует подумать о том, что выпускникам данной программы можно будет присваивать степень магистра в области юриспруденции и одновременно в области экономики инноваций и других наук. Представляется, в рамках данной программы можно было бы открыть два отделения — гуманитарное и техническое. Концептуально проработка идеи внедрения в МГУ межфакультетской магистерской программы «Информационные правоотношения в инновационной экономике» по направлению подготовки «Юриспруденция», «Экономика» и «Информационная безопасность» (далее — программа) может быть представлена следующим образом.

*Общая характеристика программы.* Целью программы является подготовка юристов нового поколения для инновационной экономики в условиях информационного общества, имеющих базовые знания в области юриспруденции, экономики и менеджмента (гуманитарное отделение); математических и алгоритмических моделей защиты информации, технологии защиты информации в современных вычислительных системах (техническое отделение). Предлагаемая программа имеет научное

и практическое значение для подготовки магистров в области правового, организационного, технического, программного и иного обеспечения информационной безопасности при производстве наукоемкой гражданской и военной продукции. Помимо фундаментальных знаний в области правоповедения, программа позволяет дать студентам специальные знания о механизмах законодательного, корпоративного и договорного регулирования в области деятельности производителей и потребителей информационной продукции (работ, услуг). Программа включает изучение взаимосвязанных с информационным правом учебных дисциплин по актуальным вопросам экономики и менеджмента инновационного производства товаров (работ, услуг) в высокотехнологичном комплексе. В учебных курсах представлены методики правового и технического сопровождения НИОКР, способы коммерциализации прав на результаты научных исследований. Отдельно раскрываются формы и методы выявления, предупреждения и пресечения правонарушений в информационной сфере, гражданско-правовые способы защиты прав на информацию, актуальные междисциплинарные вопросы обеспечения информационной безопасности в организациях.

В условиях цифровой экономики на рынке труда ощущается потребность в юристах, обладающих не только юридическими, но и экономическими и техническими знаниями, навыками управления в информационной сфере, необходимыми для успешной работы в конкретных областях инновационной деятельности. Основными направлениями деятельности выпускников программы (гуманитарное отделение) могут быть: профессиональная деятельность по правовому и аудиторскому сопровождению инновационных проектов; участие в правоохранительной и правоприменительной деятельности государственных органов в области информационных отношений, разработка и экспертиза законопроектов в информационной сфере; юридическое и аудиторское сопровождение деятельности бизнес-структур; оказание юридической помощи, консалтинговые и аудиторские услуги в информационной сфере. По мнению опрошенных руководителей и специалистов, работающих в организациях информационной сферы, углубленная подготовка юристов по экономике и менеджменту позволит им квалифицированно решать не только правовые, но и управленческие и экономические вопросы, связанные с производством, получением, распространением и защитой информации в цифровой экономике. Обеспечение безопасности информации в автоматизированных системах, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите, это техническое направление подготовки, которое требует рассмотрения с участием специалистов. По нашему мнению, выпускники-магистры по специальности «Информационные правоотношения в инновационной экономи-

ке», имеющие междисциплинарные знания, должны быть востребованы на рынке труда.

*Общая структура программы.* Программа ориентирована на подготовку специалистов, сочетающую изучение теоретических положений права, экономики и управления с одновременным формированием правовых и экономических знаний и навыков в управлении, которые позволят магистрам эффективно работать в государственных органах власти и бизнес-структурах, действующих в информационной сфере. Структурными элементами программы является наличие: общеобразовательного цикла теоретических дисциплин, нацеленных на формирование общей и профессиональной информационной культуры юриста нового поколения в условиях развития гражданского общества и правового государства; новых базовых курсов, посвященных изучению на более высоком уровне, чем в бакалавриате, актуальных вопросов информационного и других отраслей права, экономической теории и управления в инновационной экономике; учебных курсов по выбору, ориентированных на передачу студентам знаний и опыта управления с элементами экономического, организационного, технического и правового обеспечения деятельности организаций в инновационной экономике; различных форм научно-исследовательской работы (участие в конференциях, научных семинарах, подготовка магистерской диссертации и др.), что позволит студентам получить подготовку для реализации исследовательских проектов.

По нашему мнению, реализация межфакультетской магистерской программы предполагает решения следующих вопросов:

1) разработка, согласование условий и подписание договора между Юридическим факультетом, Высшей школой государственного аудита, Экономическим факультетом и Факультетом вычислительной математики и кибернетики МГУ о совместной подготовке магистров и обмене ресурсами в рамках межфакультетской магистерской программы «Информационные правоотношения в инновационной экономике»; принятие решения руководством Московского университета о возможности выдачи выпускникам магистратуры диплома МГУ по направлению подготовки «Юриспруденция» и «Экономика» (гуманитарное отделение), и «Информационная безопасность» (техническое отделение), и включение иных условий в договор, обеспечивающих реализацию межфакультетской магистерской программы в Московском университете;

2) ежегодное объявление факультетами порядка набора студентов на программу и назначение научными руководителями данной программы представителей Юридического факультета, Высшей школы государственного аудита, Экономического факультета и Факультета вычислительной математики и кибернетики МГУ;

3) утверждение научной специализации магистерской программы, выделение факультетами необходимого количества бюджетных мест

для очного обучения студентов в магистратуре, определение порядка приема в магистратуру и проведение факультетами вступительного испытания (экзамена) в соответствии с образовательными программами факультетов, участвующими в магистерской программе.

Представляется, что внедрение межфакультетской магистерской программы будет способствовать повышению уровня междисциплинарных знаний выпускников, необходимых для работы в условиях информационного общества и имиджа МГУ в эпоху цифровой экономики. Кроме того, предлагается проработка идеи о внедрении межвузовской сетевой магистерской программы по информационному праву. Автором разработан для обсуждения проект договора «О совместной образовательной программе МГУ имени М.В. Ломоносова и МГИМО МИД России» для подготовки юридических кадров в условиях мирового информационного общества и цифровой экономики (см. в этом номере журнала статью «Проект сетевой магистерской программы подготовки юристов на межвузовской платформе»).

Что касается практических рекомендаций по внедрению результатов междисциплинарных исследований, то приоритетными направлениями, на наш взгляд, являются: 1) реализация в МГУ имени М.В. Ломоносова межфакультетской магистерской программы «Информационные правоотношения в инновационной экономике»; 2) открытие на юридическом факультете межкафедрального научно-образовательного центра «Право и информация» с участием преподавателей, студентов и аспирантов юридического факультета и других факультетов МГУ (Положение о НОЦ, см.: <https://istina.msu.ru/reports/8944711/>); 3) включение научной специальности «Информационное право» в Диссертационный совет МГУ имени М.В. Ломоносова по специальности 5.1.2 «Публично-правовые (государственно-правовые) науки для подготовки научных кадров по информационному праву».

### **Литература**

1. Богатырева Е.Н. Феномен информации в контексте научного познания: философский анализ : дис. ... канд. философ. наук / Е.Н. Богатырева. Саратов, 2000. URL: <https://www.dissercat.com/content/fenomen-informatsii-v-kontekste-nauchnogo-poznaniya-filosofskii-analiz>
2. Бычкова А.М. Информационное право: статистическое исследование тематики и количества диссертационных работ по научной специальности 12.00.13 / А.М. Бычкова // Пролог: журнал о праве. 2020. № 4 (28). URL: <https://cyberleninka.ru/article/n/informatsionnoe-pravo-statisticheskoe-issledovanie-tematiki-i-kolichestva-dissertatsionnyh-rabot-po-nauchnoy-spetsialnosti-12-00-13>

3. Инновационное право : учебник / А.И. Маркеев, В.А. Свиридов, Н.М. Тюкавкин, Р.З. Юсупов / отв. ред. докт. юрид. наук, профессор А.В. Юдин. Самара : Издательство Самарского университета, 2020. 308 с.
4. Кадочников В.П. Философские проблемы научных исследований феномена информации / В.П. Кадочников // ОНВ. 2007. № 2 (54). URL: <https://cyberleninka.ru/article/n/filosofskie-problemy-nauchnyh-issledovaniy-fenomena-informatsii>
5. Лопатин В.Н. Методологические проблемы понимания и правового регулирования оборота информации / В.Н. Лопатин // Северин В.А. Актуальные вопросы правового регулирования и защиты информации в России (избранные труды). Москва, 2021. 475 с.
6. Лопатин В.Н. Информационное право : учебник для вузов. 3-е изд., с изм. и доп. / В.Н. Лопатин. Москва : Проспект, 2021. 660 с.
7. Муранов А. Юрнауки в проекте Номенклатуры научных специальностей // URL: [https://zakon.ru/blog/2020/10/08/yurnauki\\_v\\_proekte\\_nomenklatury\\_nauchnyh\\_specialnostej\\_vazhna\\_dlya\\_zaschity\\_dissertacij\\_zerkalo\\_sovr](https://zakon.ru/blog/2020/10/08/yurnauki_v_proekte_nomenklatury_nauchnyh_specialnostej_vazhna_dlya_zaschity_dissertacij_zerkalo_sovr)
8. Северин В.А. Коммерческая тайна в России : монография / В.А. Северин. Москва : Зерцало-М, 2007. 614 с.
9. Северин В.А. Коммерческая тайна в России : монография. 2-е изд., перераб. и доп. / В.А. Северин. Москва : Зерцало-М, 2009. 472 с.
10. Темы диссертаций и авторефератов по специальности ВАК РФ 12.00.14 Административное право, финансовое право, информационное право // Электронная библиотека диссертаций. URL: <https://www.dissercat.com/catalog/yuridicheskie-nauki/administrativnoe-pravo-finansovoe-pravo-informatsionnoe-pravo?page=120>

**Чижов Иван Владимирович,**

руководитель Центра проблем информационной безопасности ВМК МГУ,  
кандидат физико-математических наук  
*ichizhov@cs.msu.ru*

**Карасев Павел Александрович,**

старший научный сотрудник Центра ИПИБ, кандидат политических наук  
*karpaul@mail.ru*

**Соколов Владимир Викторович,**

заместитель руководителя Центра ИПИБ, кандидат экономических наук  
*sokolov46@yandex.ru*

**Шаряпов Ринат Абдулберович,**

ведущий научный сотрудник Центра ИПИБ, кандидат политических наук  
*sharyapovr@iisi.msu.ru*

**Яценко Валерий Владимирович,**

заместитель руководителя Центра ИПИБ, кандидат физико-математических наук

## **ЦЕНТР ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВМК МГУ: МЕЖДИСЦИПЛИНАРНЫЕ ПОДХОДЫ СПЕЦИАЛИСТОВ ДЛЯ ИННОВАЦИОННОЙ ЭКОНОМИКИ**

Процесс массового освоения информационного пространства, который начался с появлением глобальных компьютерных сетей в конце 20-го века, непрерывно ускоряется. Сейчас уже большая часть населения планеты пользуется Интернетом<sup>1</sup>. Развиваются цифровые сектора экономики, идет становление индустрии 4.0. Человечество только начинает широко использовать в своей деятельности такие инновации, как большие данные, квантовые вычисления, дополненная и виртуальная реальность, блокчейн, но при этом зачастую не задумывается о связанных с ними возможных рисках и угрозах. Необходимо фундаментальное научное осмысление и понимание происходящих процессов и прогнозирование их последствий. Эффективная работа в этой сфере невозможна без междисциплинарного подхода и объединения усилий научных коллективов различных государств.

**Ключевые слова:** междисциплинарные подходы, инновационная экономика, информационная безопасность, коммерческая тайна, коммерческое право.

<sup>1</sup> World Internet usage and Population statistics, 2021 Year-Q1 Estimates // Internet World Stats : Official website. URL: <https://www.internetworldstats.com/stats.htm>

**Ivan Vladimirovich Chizhov,**

Head of the Center for Information Security Problems  
of the Higher School of Mathematics and Cybernetics, PhD in Physics and Mathematics

**Karasev Pavel Aleksandrovich,**

Senior Researcher of the IPIB Center, PhD in Political Science

**Sokolov Vladimir Viktorovich,**

Deputy Head of the IPIB Center, PhD in Economics

**Rinat Abdulberovich Sharyapov,**

Rinat Abdulberovich Sharyapov, Leading Researcher, IPIB Center, PhD in Political Science

**Yashchenko Valery Vladimirovich,**

Deputy Head of the IPIB Center, PhD in Physics and Mathematics

## **CENTER FOR INFORMATION SECURITY PROBLEMS OF THE HIGHER SCHOOL OF ECONOMICS, MOSCOW STATE UNIVERSITY: INTERDISCIPLINARY APPROACHES OF SPECIALISTS FOR INNOVATIVE ECONOMY**

The process of mass development of the information space, which began with the appearance of global computer networks at the end of the 20th century, is constantly accelerating. Now most of the world's population is already using the Internet. Digital sectors of the economy are developing, and Industry 4.0 is emerging. Mankind is just beginning to make wide use of such innovations as big data, quantum computing, augmented and virtual reality, and blockchain, but often without thinking about the possible risks and threats associated with them. There is a need for fundamental scientific understanding and awareness of the processes taking place and predicting their consequences. Effective work in this area is impossible without an interdisciplinary approach and combining the efforts of scientific teams from different countries.

**Keywords:** interdisciplinary approaches, innovation economy, information security, trade secrets, commercial law.

### **История и достижения**

В Московском университете с начала 90-х годов прошедшего столетия проводились научные исследования и образовательные программы по защите информации и информационной безопасности. Мощным импульсом к дальнейшему развитию этого направления научно-образовательной деятельности стало принятие в июле 2000 г. лидерами стран

Группы восьми (G8) «Окинавской хартии глобального информационного общества»<sup>2</sup>, инициатором принятия которой был Президент России В.В. Путин. Ректор МГУ академик В.А. Садовничий приложил огромные усилия по внедрению идей этого документа в деятельность МГУ и сделал многое, чтобы они получили развитие на государственном уровне. В сборнике «Научные проблемы национальной безопасности Российской Федерации» (издается Советом Безопасности Российской Федерации) была опубликована статья академика В. Садовниченко «Как защитить человека от инфогенных рисков и угроз?»<sup>3</sup>, в которой было отмечено, что «долг научно-образовательной корпорации — разработать и внедрить систему знаний, навыков и норм глобальной культуры информационной безопасности». Эта статья распространялась на съезде Союза ректоров России, переведена на английский, китайский, корейский и японский языки, была передана ректорам ряда российских и зарубежных университетов — партнеров МГУ и вызвала большой резонанс в международном научно-образовательном сообществе.

В 1999 г. по инициативе ректора Московского университета академика В.А. Садовниченко и первого заместителя Секретаря Совета Безопасности Российской Федерации В.П. Шерстюка было положено начало активным исследованиям проблематики информационной безопасности на всех факультетах МГУ. Под их руководством в 2000 г. начал свою работу ежеквартальный межведомственный и межфакультетский семинар «Научные проблемы информационной безопасности». По решению Ученого совета Московского университета на все факультеты МГУ был направлен перечень направлений научных исследований по тематике информационной безопасности, рекомендованных для использования в учебном процессе и научных изысканиях, в том числе и для написания курсовых и дипломных работ.

Летом 2001 г. в МГУ совместно с представителями США была проведена первая в истории международная конференция по информационной безопасности, собравшая около 500 участников из более чем 45 стран<sup>4</sup>. В проведении Конференции участвовало более 10 факультетов МГУ.

В октябре 2002 г. в МГУ была проведена межведомственная научная конференция «Московский университет и развитие криптографии в России», которая стала первой в цикле ежегодных конференций по тематике информационной безопасности и противодействия терроризму.

<sup>2</sup> Окинавская хартия Глобального информационного общества (принята 21 июля 2000 года) // URL: <http://www.kremlin.ru/supplement/3170>

<sup>3</sup> Садовничий В.А. Как защитить человека от инфогенных рисков и угроз? // Научные проблемы национальной безопасности Российской Федерации. Вып. 5: К 20-летию образования Совета Безопасности Российской Федерации. М., 2012. С. 299.

<sup>4</sup> Интервью с заместителем директора Института проблем информационной безопасности МГУ В.В. Яценко // Компьютерра. 2006. № 47–48. С. 9–10.



В результате этих инициатив с 1999 по 2003 г. на ряде факультетов Московского университета были созданы кафедры и лаборатории, а также разработаны учебные курсы по тематике информационной безопасности. В 1999 г. на факультете дополнительного образования МГУ была создана кафедра информационной безопасности.

В этой связи ректор Московского университета академик В.А. Садовничий принял решение о создании центра, координирующего проводимые в МГУ исследования по проблематике информационной безопасности. В качестве обособленного структурного подразделения университета в 2003 г. был организован Институт проблем информационной безопасности (ИПИБ МГУ) во главе с В.П. Шерстюком. Открытие Института явилось результатом долговременных и результативных междисциплинарных исследований в области информационной безопасности, проводимых различными научными коллективами Московского университета.

Синергия естественных, технических и гуманитарных наук нашла отражение в структуре Института, в виде трех отделов: математических проблем информационной безопасности, информационной безопасности компьютерных систем и гуманитарных проблем информационной безопасности. В число основных задач нового подразделения вошли: определение направлений исследований, проведение фундаментальных и прикладных научных исследований по проблемам информационной безопасности; участие в международном научном и научно-педагогическом сотрудничестве по проблемам информационной безопасности; научно-пропагандистская деятельность с целью широкого распространения научных основ безопасности жизнедеятельности в информационном обществе. Для реализации этих задач было налажено взаимодействие с факультетами и задействованы международные связи университета, организовывались и проводились международные научные конференции и семинары — общероссийские научные конференции «Математика и безопасность информационных технологий», международные научные конференции по проблемам безопасности и противодействия терроризму. ИПИБ в сотрудничестве с международными партнерами МГУ организовывал многочисленные зарубежные мероприятия на территории стран Европы, Азии и Америки, в том числе в бывших республиках СССР. Результаты проведенных мероприятий докладывались заинтересованным органам исполнительной власти; также публиковались материалы конференций в виде сборников докладов и научных статей. В программу мероприятий включались доклады по широкому спектру научных направлений — математических, компьютерных, философских, политологических, психологических. Также в ряде структурных подразделений МГУ начали функционировать кафедры и лаборатории по этой тематике, проводятся научные конференции, в том числе и международные. В 2013 г. приказом ректора

Московского университета В.А. Садовниченко была создана кафедра информационной безопасности факультета ВМК МГУ.

Научный потенциал ИПИБ МГУ посредством консультаций и аналитических докладов был задействован при разработке многих доктринальных документов и документов стратегического планирования Российской Федерации, в частности, Доктрины информационной безопасности<sup>5</sup> и Основ государственной политики Российской Федерации в области международной информационной безопасности<sup>6</sup>. Институт также принимал участие в разработке Концепции Конвенции ООН об обеспечении международной информационной безопасности<sup>7</sup>.

Опыт, полученный при проведении зарубежных мероприятий, позволил ИПИБ при поддержке аппарата Совета Безопасности Российской Федерации и Министерства иностранных дел Российской Федерации в сотрудничестве с российскими и зарубежными партнерами на протяжении многих лет организовывать и проводить международные научные форумы «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» в немецком городе Гармиш-Партенкирхен. Форум занял особое место среди организованных Институтом мероприятий и стал одним из наиболее значимых его достижений. Этот форум, получивший в СМИ наименование «Электронный Давос», проводился в Германии ежегодно с 2007 по 2019 г. Московскому университету вместе со своими партнерами удалось создать уникальную площадку, где международный междисциплинарный коллектив ученых, специалистов и политиков может не только открыто высказывать и выслушивать разные точки зрения, но и приложить свой интеллектуальный и экспертный потенциал для поиска общих ответов на общие проблемы. Круглые столы по вопросам управления Интернетом, атрибуции, противодействия экстремизму и терроризму в ИКТ-среде объединяли за одним столом представителей различных отраслей знания — компьютерных специалистов, математиков, юристов и политологов. На этом мероприятии с участием дипломатов и военных экспертов также обсуждались взаимоотношения России и западных государств по вопросам безопасности в информационном пространстве. Результаты конференций докладывались высшему руководству страны

<sup>5</sup> Доктрина информационной безопасности Российской Федерации : утв. Указом Президента РФ № 646 от 5 декабря 2016 г. // Официальный сайт Совета Безопасности Российской Федерации. URL: <http://scrf.gov.ru/security/information/document5/>

<sup>6</sup> Основы государственной политики Российской Федерации в области международной информационной безопасности : утв. Указом Президента Российской Федерации от 12 апреля 2021 г. № 213 // Официальный сайт Совета Безопасности Российской Федерации. URL: <http://scrf.gov.ru/security/information/document114/>

<sup>7</sup> Концепция Конвенции ООН об обеспечении международной информационной безопасности // Официальный сайт Совета Безопасности Российской Федерации. URL: <http://scrf.gov.ru/security/information/document112/>

и активно использовались на площадке ООН для доведения позиции России по различным аспектам формирования системы международной информационной безопасности (МИБ). После начала пандемии COVID-19 было принято решение о проведении очередного Форума в онлайн-формате в Москве. Несмотря на сложившуюся эпидемиологическую и политическую обстановку, в работе XIV Международного форума по проблемам международной информационной безопасности приняли участие более 120 экспертов из 12 государств. Было представлено более 60 докладов по различным аспектам налаживания сотрудничества в области противодействия угрозам безопасности использования информационных и коммуникационных технологий человеком, коммерческими и некоммерческими организациями, государственными органами<sup>8</sup>.

Форум в Гармиш-Партенкирхене, организация которого является самостоятельным достижением, стала местом реализации ряда проектов. Так, в 2010 г. здесь был организован Международный исследовательский консорциум информационной безопасности (МИКИБ), в который изначально вошли 11 организаций из 9 стран. Одной из функций МИКИБ стала интенсификация профильных обсуждений: эксперты получили возможность участвовать в семинарах по отдельным проблемам МИБ, которые проводились в «межгармишевский» период по приглашению участников МИКИБ в их странах. Многие научные и бизнес-структуры проявили интерес к работе Консорциума, и со временем число участников достигло 28 организаций из 18 стран. Одним из значимых достижений МИКИБ стала реализация проекта, посвященного проработке отдельных вопросов применения международного права в ИКТ-среде. Под руководством профессора А.А. Стрельцова и международного коллектива специалистов (из России, США, Эстонии и Швейцарии) была подготовлена монография «Методологические вопросы применения норм, правил и принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды»<sup>9</sup>. Разработка научно-методического подхода к применению добровольных и необязательных норм, правил и принципов ответственного поведения государств направлена на содействие формированию некоторого стандарта поведения государств в рассматриваемой области.

<sup>8</sup> XIV международный Форум по проблемам международной информационной безопасности : расширенный пост-релиз // НАМИБ : официальный сайт. URL: <https://namib.online/2020/12/rasshirenyj-post-reliz-xiv-mezhdunarodnyj-forum-po-problemam-mezhdunarodnoj-informacionnoj-bezopasnosti/>

<sup>9</sup> Методологические вопросы применения норм, правил и принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной ИКТ-среды // НАМИБ : официальный сайт. URL: <https://namib.online/2020/07/metodologicheskie-voprosy-primenenija-norm-pravil-i-principov-otvetstvennogo-povedenija-gosudarstv-prizvannyh-sposobstvovat-obespecheniju-otkrytoj-bezopasnoj-stabilnoj-dostupnoj-i-mirnoj-ikt-sredy/>

Большую пользу международному сотрудничеству, в частности между Россией и США, принесла реализация МГУ совместного проекта по критически важной терминологии с американским Институтом Восток — Запад. Эта работа позволила получить две публикации (в 2011 и 2013 гг.) с важнейшими согласованными терминами в области международной информационной безопасности. Термины, которые имеют одинаковый смысл для каждой участвующей в переговорах стороны, являются строительным материалом для международных соглашений. Выработка подобного глоссария необходима, поскольку ИКТ-среда отличается от любой другой области взаимодействия степенью сложности, скоростью развития, а также тем, что вбирает в себя множество ключевых концепций, которые зачастую находятся за пределами понимания дипломатов, не имеющих глубокой технической подготовки.

В апреле 2018 г. при содействии Совета Безопасности Российской Федерации Московский государственный университет имени М.В. Ломоносова, Московский государственный институт международных отношений (Университет) МИД России, Дипломатическая академия МИД России, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Институт современных проблем безопасности (ГМК «Норильский никель») и редакция журнала «Международная жизнь» (МИД России) учредили Национальную Ассоциацию международной информационной безопасности (НАМИБ). По инициативе ректора МГУ академика Виктора Антоновича Садовниченко учредительное собрание Ассоциации состоялось в Главном здании Московского университета. Президентом Ассоциации был избран директор ИПИБ В.П. Шерстюк. В состав Президиума Ассоциации входят, в частности, специальный представитель Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, Чрезвычайный и Полномочный Посол Российской Федерации Андрей Крутских, вице-президент Группы компаний «Цитадель» Борис Мирошников, начальник департамента аппарата Совета Безопасности Российской Федерации Сергей Бойко и другие известные специалисты в области обеспечения информационной безопасности<sup>10</sup>.

### Перспективы

В настоящее время в Московском университете по инициативе ректора академика В.А. Садовниченко и при поддержке Председателя попечительского Совета Президента Российской Федерации В.В. Путина проводится большая работа по концентрации усилий научного потенциала Университета на решении важнейших проблем развития современного

<sup>10</sup> Члены президиума НАМИБ // НАМИБ : официальный сайт. URL: <https://namib.online/chleny-prezidiuma/>

общества. Тематику информационной безопасности возглавил факультет вычислительной математики и кибернетики МГУ, обладающий колоссальными теоретическими и практическими наработками в области информационных технологий и, в частности, компьютерной безопасности. Факультет объединил свои усилия с Институтом проблем информационной безопасности, создав научный Центр проблем информационной безопасности. С учетом кадровых перестановок, осуществленных после создания НАМИБ, руководителем Центра был назначен И.В. Чижов, доцент кафедры информационной безопасности ВМК.

На сегодняшний момент Центр ИПИБ отвечает в МГУ за развитие и реализацию темы «Безопасность информационного пространства: междисциплинарная диагностика и обеспечение». Междисциплинарность в проведении научных исследований и реализации образовательных программ — одно из важнейших условий решения проблем безопасности информационного пространства. На факультете ВМК в этом году начинается междисциплинарное обучение по направлению «Информационная безопасность», на факультете разработаны спецкурсы гуманитарной направленности, началось составление соответствующих учебно-методических пособий. Уже привлечены специалисты в области политологии, экономики и международных отношений, в дальнейшем планируется задействовать психологов, юристов и представителей факультета журналистики. Также начата проработка межфакультетских магистерских программ, в том числе с факультетом государственного управления и с юридическим факультетом. Предполагается, что, обладая междисциплинарными компетенциями, выпускники программ смогут на качественно новом уровне и с пониманием предмета решать поставленные перед ними задачи. Так, например, невозможно осуществить юридическую проработку использования биткойна, не понимая, что собой представляет технология блокчейна.

Есть ряд проблем как на национальном, так и на международном уровне, для решения которых необходим междисциплинарный подход, а также подготовка высококвалифицированных кадров с необходимыми компетенциями.

### ***1. Атрибуция инцидентов в киберпространстве и формирование «цифровых границ» зон ответственности государств за инциденты в киберпространстве.***

Из-за нерешенности этой проблемы виновные в трансграничных масштабных кибератаках до сих пор не выявляются, а «назначаются», как правило, из политических соображений. Для ее решения необходимы серьезные компетенции в следующих областях:

- строение и функционирование сети «Интернет»;
- теория международных отношений;

- международное право;
- особенности криминализации киберпреступлений в различных странах, и т.д.

## **2. Выявление на ранних этапах многоходовых информационно-политических операций.**

Из-за нерешенности этой проблемы начинает работать теорема Томаса из области социальной психологии. Классик американской социологии Уильям Айзек Томас еще в 1923 г. сформулировал постулат: «Если люди определяют ситуации как реальные, они реальны по своим последствиям». Политическая практика многих государств свидетельствует о том, что этот постулат верный. Наряду с субъективной и объективной реальностью, сформировалась «третья реальность» — глобальная медиасфера, через которую можно оказывать влияние на принятие решений и поступки людей. Та реальность, которая выходит за пределы повседневных проблем, забот и интересов обывателей, посредством медиасферы замещается представлением об этой реальности. После этого все последствия сформированного представления о ситуации люди будут считать правильными<sup>11</sup>.

Именно эта закономерность используется при разработке и проведении информационных операций. По своей структуре они многоходовые, то есть в нужный момент развертывается очередная кампания по «обновлению» медиасобытия. Возникают цепочки фейков, которые взаимодополняют и усиливают друг друга. Воздействие осуществляется не только в горизонтальной плоскости, но и в вертикальной — начиная от простых обывателей и заканчивая самыми верхними уровнями власти. В тот момент, когда искаженное представление о действительности внедряется в умы политиков, искоренить его становится гораздо сложнее. Поэтому так важно научиться выявлять информационные кампании на самых ранних этапах их развертывания и купировать распространение фейков.

Для ее решения необходимы серьезные компетенции в следующих областях:

- политология;
- информационное противодействие (противоборство);
- политическая социология;
- социальная психология;
- политическая культура и идеология;
- журналистика;
- медиакommunikации;
- политическая коммуникативистика.

<sup>11</sup> Карасев П.А., Шаряпов Р.А., Яшенко В.В. Контент в новых медиа как инструмент вмешательства во внутренние дела суверенных государств // Международная жизнь. 22.02.2019. URL: <https://interaffairs.ru/news/show/21739>

### ***3. Формирование массовой культуры кибербезопасности.***

Очевидно, что продолжающееся массовое освоение информационного пространства приводит как к позитивным, так и к негативным последствиям, в том числе появлению новых вызовов и угроз. Противодействовать им необходимо не только на уровне государства и общества, но и на уровне простых пользователей, с пониманием того, что отдельный человек — самое базовое звено в цепи обеспечения информационной безопасности. Нередко он же — самое слабое звено. К сожалению, массовое освоение ИКТ-среды не влечет за собой автоматическое формирование массовой культуры кибербезопасности — такого состояния, при котором каждый пользователь обладает достаточным уровнем компьютерной грамотности и соблюдает при этом определенные правила кибергигиены. Из-за нерешенности этой проблемы злоумышленникам не составляет труда осуществлять свою вредоносную кибердеятельность, в том числе с использованием приемов социальной инженерии. Ликвидация безграмотности в области информационной безопасности — острая и глобальная задача, для решения которой необходимо объединение усилий государства и бизнеса, гражданского общества и образовательных учреждений. В образовательной среде задача формирования массовой культуры кибербезопасности должна решаться не только вертикально — со школьной скамьи и до вузов, но и горизонтально — по всем направлениям подготовки специалистов.

Для ее решения необходимы компетенции в следующих областях:

- информационно-коммуникационные технологии;
- информационная безопасность;
- политология;
- социальная философия;
- конфликтология
- культурология.

### ***4. Формирование массового иммунитета к пропаганде (через социальные сети) терроризма и к вовлечению в террористическое подполье.***

Интернет и сетевые технологии являются особенно мощными инструментами в руках экстремистских и террористических группировок, которые используются для распространения идеологии насильственного экстремизма и терроризма и рекрутинга в ряды сторонников джихада. Известно, что члены ИГИЛ (террористическая организация, запрещенная в России) использовали возможности веб-технологий для создания глобальной международной террористической сети, а мессенджеры и социальные сети — для пропаганды своих идей и вербовки новых членов. По мере развития технологий и расширения информационного поля сложность противодействия угрозам пропаганды насильственного экстремизма и идеологии терроризма сохраняется и углубляется. Отсутствие массового иммунитета к деструктивной пропаганде приводит к тому, что

все большее число граждан, особенно молодежи, находится в зоне риска. Решить эту проблему только при помощи национальных регулятивных (включая запретительные) правовых норм невозможно, в том числе потому, что идеология терроризма и экстремизма зачастую распространяется вне регулируемого информационного поля. Когнитивных способностей человека сегодня уже недостаточно, чтобы адекватно осознавать весь поступающий поток информации, и поэтому уязвимости человеческого сознания могут быть использованы для «промыывания мозгов». Для выработки методик и подходов к «когнитивной иммунизации» необходима работа многих специалистов — психологов, социологов, лингвистов.

Для ее решения необходимы серьезные компетенции в следующих областях:

- строение и функционирование социальных сетей как составной части сети «Интернет»;
- когнитивные психология, социология и лингвистика;
- политическая культура и идеологии;
- политическая коммуникация;
- религиоведение.

##### ***5. Формирование массового иммунитета к размыванию (через социальные сети) традиционных российских ценностей.***

В Доктрине информационной безопасности Российской Федерации<sup>12</sup> отмечается, что под влиянием внешних акторов религиозные, этнические, правозащитные и иные организации активно оказывают информационно-психологическое воздействие, направленное на дестабилизацию внутривнутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств, при этом широко используются возможности информационных технологий. Нарастает информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей. Так, в мае 2021 г. на заседании оргкомитета «Победа» Президент России Владимир Путин заявил, что в последнее время участились попытки оболгать и извратить историю Великой Отечественной войны, в том числе «промыть мозги» молодым россиянам<sup>13</sup>. Из-за нерешенности этой проблемы происходит глубокое расщепление российского общества и антагонизация интересов отдельных социально-культурных групп по отношению к национальному метакультурному коду. Идет размывание идеи многонационального народа Российской Федерации, соединенно-

<sup>12</sup> Доктрина информационной безопасности Российской Федерации : утв. Указом Президента РФ № 646 от 5 декабря 2016 г. // Официальный сайт Совета Безопасности Российской Федерации. URL: <http://scrf.gov.ru/security/information/document5/>

<sup>13</sup> Заседание Российского организационного комитета «Победа» 20 мая 2021 года // Официальный сайт Президента России. URL: <http://www.kremlin.ru/events/councils/65618>



го общей судьбой на своей земле. Как в случае с пропагандой терроризма и экстремизма, объектом деструктивного воздействия является сознание индивида, а значит, бороться с этой угрозой исключительно запретительными и иными регулятивными методами неэффективно.

Для ее решения необходимы серьезные компетенции в следующих областях:

- история;
- социальная философия;
- культурология;
- теория и практика межкультурной коммуникации;
- социальная психология;
- религиоведение;
- организация работы с молодежью;
- строение и функционирование социальных сетей как составной части сети «Интернет».

Междисциплинарный научный подход — это ключ к решению актуальных проблем информационной безопасности. Однако ведущая роль высшей школы в этом вопросе опирается не только на науку, но и на обеспечение междисциплинарного образования. В МГУ сформированы научно-образовательные школы, задача которых развитие наиболее перспективных междисциплинарных направлений современной науки, объединение учебного процесса и научных исследований на всех образовательных уровнях, а также создание новых уникальных междисциплинарных образовательных программ, подготовка высококвалифицированных кадров. Эти надфакультетские объединения призваны на практике продемонстрировать эффективность междисциплинарности. Наука и образование вместе должны дать инструментарий для решения поставленных задач — научно-обоснованные рекомендации, широкий спектр специальных образовательных программ, методик преподавания, учебной и научно-популярной литературы.

С 2017 г. факультет ВМК МГУ активно сотрудничает с юридическим факультетом МГУ в реализации междисциплинарного подхода к обучению студентов магистратуры. Начальник Центра ПИБ И.В. Чижов читает курс лекций «Корпоративные системы защиты информации в организациях» для студентов второго года магистратуры, обучающихся на юридическом факультете МГУ по программе «Информационные правоотношения в инновационной экономике» (руководитель — профессор В.А. Северин, д.ю.н.). Эта магистерская программа, по существу, является междисциплинарной межфакультетской программой МГУ. В рамках курса «Корпоративные системы защиты информации в организациях» студенты, которые получают гуманитарное образование, знакомятся с особенностями работы технических средств защиты информации,

изучают базовые математические методы, используемые в реализации этих средств защиты. В частности, они знакомятся:

- с терминологией в области технической защиты информации;
- с требованиями к системам и средствам защиты информации от несанкционированного доступа;
- с основными российскими и международными стандартами в области защиты информации;
- с методами противодействия разрушающим программным компонентам;
- с базовыми типами уязвимостей программного обеспечения;
- базовыми методами и средствами сетевой безопасности;
- с подходами и основными особенностями к построению систем в защищенном исполнении;
- с научно-технической литературой в области построения средств защиты информации автоматизированных систем;
- с основной нормативной базой в области защиты информации.

В курсе рассматриваются особенности современных корпоративных информационных систем. Требования к системам и средствам защиты информации от несанкционированного доступа. Классификация автоматизированных систем и требования по защите информации. Показатели защищенности средств вычислительной техники. Соответствие классов систем различным уровням конфиденциальности. Понятие модели нарушителя информационной безопасности и модели угроз информационной безопасности. Политика безопасности. Принципы построения системы защиты информации. Подходы к определению уязвимостей автоматизированных систем и выбор средств защиты. Формирование требований к построению систем защиты. Создание автоматизированных систем в защищенном исполнении.

Слушатели знакомятся с базовыми моделями разграничения доступа в компьютерных системах: дискреционное, мандатное управления доступом. Методами контроля доступа к ресурсам компьютерной системы. Изучают основные типы разрушающих программных воздействий и знакомятся с особенностями защиты от них. Рассматривают уязвимости приложений и атаки типа «отказ в обслуживании», а также базовые методы криптографической защиты интернет-соединений.

Особое место в курсе уделяется вопросам электронного документооборота, так как юристы, работающие в области защиты информации, в первую очередь должны уметь ориентироваться в современных подходах к обеспечению юридической силы электронных документов. В курсе вводятся важнейшее понятие юридической значимости документа. Подробно рассматривается федеральный закон об электронной подписи в разрезе упоминаемых в нем технологий.

В последние годы в рамках курса подробно разбираются основы технологии блокчейн и ее применения для построения криптовалют.

Каждый год курс «Корпоративные системы защиты информации в организациях» получает только положительные отклики от студентов магистратуры.

Центр проблем информационной безопасности, как структурная единица ВМК, в полной мере участвует в работе научно-образовательной школы «Мозг, когнитивные системы, искусственный интеллект». Миссия этой школы — обеспечение прогресса в решении фундаментальных задач, связанных с раскрытием природы когнитивных систем, пониманием принципов работы мозга и созданием систем искусственного интеллекта, позволяющих существенно ускорить научно-технический прогресс, улучшить когнитивные возможности и здоровье человека<sup>14</sup>. Реализация этой миссии невозможна без применения междисциплинарного подхода, и Центр, обладая колоссальным опытом реализации межфакультетских проектов с привлечением всех отраслей знания, способен в значительной степени способствовать ее реализации.

### Литература

1. Интервью с заместителем директора Института проблем информационной безопасности МГУ В.В. Ященко // Компьютерра. 2006. № 47–48. С. 9–10.
2. Карасев П.А. Контент в новых медиа как инструмент вмешательства во внутренние дела суверенных государств / П.А. Карасев, Р.А. Шаряпов, В.В. Ященко // Международная жизнь. 22.02.2019. URL: <https://interaffairs.ru/news/show/21739>
3. Садовничий В.А. Как защитить человека от инфогенных рисков и угроз? / В.А. Садовничий // Научные проблемы национальной безопасности Российской Федерации. Вып. 5: К 20-летию образования Совета Безопасности Российской Федерации. Москва, 2012. С. 299.

<sup>14</sup> Мозг, когнитивные системы, искусственный интеллект // Научно-образовательные школы МГУ. URL: <https://nosh.msu.ru/brain>

**Иващенко Наталия Павловна,**  
заведующий кафедрой экономики инноваций,  
заместитель декана по межфакультетскому взаимодействию  
и инновационной деятельности,  
Экономический факультет МГУ имени М.В. Ломоносова,  
доктор экономических наук, профессор  
*nivashenko@mail.ru*

## **РОЛЬ ЭКОНОМИЧЕСКИХ ЗНАНИЙ В ПОДГОТОВКЕ ЮРИДИЧЕСКИХ КАДРОВ ДЛЯ ИННОВАЦИОННОЙ ЭКОНОМИКИ**

В статье анализируется роль Московского университета, выполняющего социально значимую роль в образовании и науке, который принял на себя новую миссию и сформулировал цели общества по развитию научно-технической и инновационной модернизации России. Государственная политика вовлечения университетов в инновационную и внедренческую деятельность способствует развитию кооперации вузов с бизнес-средой, созданию малых инновационных предприятий, имеющих целью коммерческое применение вузовских разработок. Примером для других университетов является Московский университет, который прошел путь трансформаций — от создания Научного парка (1991 г.) и ключевых элементов инновационной инфраструктуры до образования на территории МГУ Инновационного научно-технологического центра «Воробьевы горы» (2013 г.), что, по замыслу ректора Московского университета академика В.А. Садовниченко, должно обеспечить формирование полноценной инновационной экосистемы, включая новые исследовательские центры и специализированную инфраструктуру для научно-технологической деятельности.

Значительную роль в движении Московского университета по инновационному пути развития играет экономический факультет, где впервые были разработаны концептуальные теоретические основы инновационной экономики, создан инновационный кластер, включающий кафедру экономики инноваций, Бизнес-клуб МГУ, Студенческий бизнес-инкубатор МГУ, Лабораторию инновационного бизнеса и предпринимательства, Центр развития молодежного предпринимательства, Центр биоэкономики и эко-инноваций и другие структуры, сформирован творческий коллектив ученых и специалистов, которые оказывают помощь другим факультетам в формировании внутренней инновационной среды (разработаны совместные межфакультетские магистерские программы и учебные программы, учебники и пособия, читаются курсы лекций).

Ректор Московского университета В.А. Садовничий, характеризуя новый этап в развитии Московского университета, четко обозначил ключевые тенденции современного этапа развития МГУ, который связан с пониманием того, что вся современная научная работа ведется на междисциплинарном уровне, на стыке разных наук, а отсутствие готовых многопрофильных специалистов требует создания новых междисциплинарных образовательных программ. Автор обосновывает актуальность инновационного образования

и подготовки кадров нового типа на основе междисциплинарного подхода, подчеркивает важность взаимодействия экономического и юридического факультетов в рамках межфакультетской магистерской программы «Информационные правоотношения в инновационной экономике» в целях подготовки студентов к использованию экономических знаний в сфере правового обеспечения инновационной деятельности в условиях информационного общества и цифровой экономики, необходимости защиты прав граждан, юридических лиц и публично-правовых образований на результаты интеллектуальной деятельности.

**Ключевые слова:** инновационная экономика, инновационная деятельность, информационные правоотношения, инновационная среда, инновационный кластер, экономические знания, межфакультетская магистерская программа.

**Natalia P. Ivaschenko**

Head of the Department of Economics of Innovation,  
Deputy Dean for Interfaculty Cooperation and Innovation Activities,  
Faculty of Economics the Lomonosov Moscow State University  
Doctor of Economics, Professor

## **ROLE OF ECONOMIC KNOWLEDGE IN TRAINING LEGAL STAFF FOR INNOVATIVE ECONOMY**

The article analyzes the importance of Moscow University, which plays a socially significant role in education and science, which has assumed a new mission and formulated the goals of society for the development of scientific, technical and innovative modernization of Russia. The state policy of involving universities in innovation and implementation activities contributes to the development of cooperation between universities and the business environment and the creation of small innovative enterprises aimed at the commercial application of university developments. An example for other universities is Moscow University, which has gone through the path of transformations — from the creation of the Science Park (1991) and key elements of the innovation infrastructure, to the formation of the Vorobyovy Gory Innovation Science and Technology Center on the territory of Moscow State University (2013), which, according to the plan Rector of Moscow University Academician V.A. Sadovnichy must ensure the formation of a full-fledged innovation ecosystem, including new research centers and specialized infrastructure for scientific and technological activities.

A significant role in the movement of Moscow University along an innovative path of development is played by the Faculty of Economics, where the conceptual theoretical foundations of an innovative economy were first developed, an innovative cluster was created, including the Department of Economics of Innovation, the Business Club of Moscow State University, the Student Business Incubator of Moscow State University, the Laboratory of Innovative Business and Entrepreneurship, Center for the Development of Youth Entrepreneurship, Center for Bioeconomics and Eco-Innovation, and other structures; a creative team of scientists and specialists has been formed to assist other faculties in the formation of an internal innovative environment (joint interfaculty master's programs and curricula, textbooks and manuals have been developed, lecture courses are given).

Rector of Moscow University V.A. Sadovnichy, characterizing a new stage in the development of Moscow University, clearly outlined the key trends of the current stage of development of Moscow State University, which is associated with the understanding that all modern scientific work is carried out at an interdisciplinary level, at the intersection of different sciences, and the lack of ready multidisciplinary specialists requires the creation of new interdisciplinary educational programs. The author substantiates the relevance of innovative education and training of a new type of personnel on the basis of an interdisciplinary approach, emphasizes the importance of interaction between the Faculty of Economics and Law within the framework of the interfaculty master's program "Information Legal Relations in an Innovative Economy" in order to prepare students for the use of economic knowledge in the field of legal support for innovation in information society and digital economy, the need to protect the rights of citizens, legal entities and public law entities to the results of intellectual activity.

**Keywords:** innovative economy, innovative activity, information legal relations, innovative environment, innovative cluster, economic knowledge, interfaculty master's program.

### **Инновационный вектор развития Московского университета**

В условиях новой экономики, основанной на знаниях и цифровых технологиях, чрезвычайно возрастает роль образования и как инструмента развития всех сторон общества. В системе создания общественного богатства, в основе которого *образование, исследования и инновации*, ключевыми становятся организации, производящие новые знания, связанные с исследованиями и разработками, а также обеспечивающие распространение знаний и поиск путей их практического использования — научно-исследовательские институты, университеты, лаборатории, научно-производственные подразделения компаний, малые инновационные компании и др. При этом успех страны зависит не только от наличия новых идей и прорывных технологий, но и от того, насколько быстро эти технологии коммерциализируются на рынке, превращаются в новые продукты. Эта задача стала приоритетной для ведущих экономик мира.

Многие исследования последнего времени посвящены вопросу *новой роли университетов*, которые рассматриваются как один из ключевых инструментов поддержки и усиления инновационного развития. Сегодня университеты во всем мире проходят этап существенной трансформации: наряду с *обучением и исследованием* (первая и вторая функции университетов) университеты приобретают третью функцию — *инновационно-предпринимательскую*, связанную с коммерциализацией результатов научно-исследовательской деятельности<sup>1</sup>. Появление и развитие таких концепций, как *предпринимательская наука*<sup>2</sup>, *академический капитализм*<sup>3</sup>, модель гло-

<sup>1</sup> Ивашенко Н.П., Поспелова Т.В. Процесс формирования предпринимательских университетов в России // МИР (Модернизация. Инновации. Развитие). 2013. № 4 (2(14)). С. 66–70.

<sup>2</sup> Etzkowitz H. Networks of Innovation: science, technology and development in the triple helix era // Research Policy. 2002. Vol. 14 (2).

<sup>3</sup> Slaughter, S., Leslie, L.L. Academic capitalism. Politics, policies and the entrepreneurial university. Baltimore — London : The Johns Hopkins University Press, 1999.

бального научно-исследовательского университета (globalresearchuniversity) и др., свидетельствует об изменении концептуальных подходов в направлении коммерческой ориентации академической среды<sup>4</sup>, когда университеты становятся активными игроками не только в производстве *новых знаний*, но и в их распространении и использовании через *инновационную деятельность*. Предпринимательская деятельность университетов проявляется как в создании малых университетских инновационных компаний<sup>5</sup>, так и во взаимодействии университетов с компаниями из промышленности. Также в последние годы значительно возрастает интерес студентов к участию в предпринимательской деятельности, создании университетских стартапов, спин-оффов (spin-off) и т.д.

В инновационных механизмах, с помощью которых интеллектуальный продукт превращается в промышленный, участвуют как минимум три компонента — *наука (и образование), промышленность (и бизнес), государство*.

Методологической основой осуществления такого взаимодействия может рассматриваться концепция «тройной спирали» (Triple Helix), предложенная Г. Ицковичем (2000, H. Etzkovitz), которая исходит из перспективной роли университета как лидера отношений с бизнесом и государством.

Таким образом, современный университет — это не только центр подготовки кадров и реализации научных исследований, но и центр формируется современная институциональная среда, порождающая бизнесы, компании, технологии, продукты, которые потом активно востребуются рынком.

Несомненно, что эти общемировые тенденции должны были найти свое отражение и в российской практике. За последние десятилетия, исходя из лучшего мирового опыта, в стране был реализован целый ряд важнейших направлений государственной политики, способствующих развитию инновационной сферы. Особое значение имеет вовлечение вузов в инновационную и внедренческую деятельность, развитие кооперации вузов с бизнес-средой в рамках создания вузовских малых инновационных предприятий, имеющих целью коммерческое применение вузовских разработок (№ 217-ФЗ от 2 августа 2009 г.), а также развитие стратегического взаимодействия вузов с промышленными предприятиями (ППРФ № 218 от 9 апреля 2010 г.). Важно отметить правительственные инициативы по формированию в ведущих вузах современной инновационной инфраструктуры (ППРФ № 219 от 9 апреля 2010 г.), являющейся основой для развития предпринимательских компетенций обучающейся молодежи и в целом повышения инновационной активности.

Однако несмотря на то что инновационная деятельность для подавляющего числа ведущих университетов мира являлась неотъемлемой частью их

<sup>4</sup> Anderson, 2001; Lehrer and Asakawa, 2004b; Lockett et al., 2005.

<sup>5</sup> Clark, B. Sustaining Change in Universities: Continuities in Case Studies and Concepts. Open University Press, 2004. 220 p.

деятельности, постановка вопроса о развитии инновационной деятельности в российских вузах воспринималась неоднозначно. За прошедшие годы Московский университет прошел долгий путь трансформаций — от создания Научного парка (1991) и Управления инновационной политики (2004) до изменения Устава МГУ (включение пункта об инновационной деятельности, 2008) и создания ключевых элементов инновационной инфраструктуры (Программа развития МГУ до 2020 г., 2010).

2013 год мы рассматриваем как важный рубеж в развитии инновационной политики МГУ. Принятое в 2013 г. решение о создании на территории МГУ Инновационного научно-технологического центра «Воробьевы горы» должно обеспечить формирование полнокровной инновационной экосистемы, включая новые исследовательские центры и специализированную инфраструктуру для научно-технологической деятельности. Благодаря этому проекту будет создана модель особого статуса инновационных центров, своего рода университетских территорий опережающего развития. Такая модель университетских «технологических долин» впоследствии будет применяться и в других регионах страны — там, где есть развитая научная и интеллектуальная среда.

Таким образом, Московский университет принял на себя новую миссию и сформулировал новую роль в обществе — не только как субъекта, выполняющего социально значимую роль в образовании и науке, но и как важнейшего субъекта в научно-технической и инновационной модернизации России.

### **О роли экономического факультета в формировании инновационной среды Московского университета**

Активная инновационная политика Московского университета этого периода дала мощный импульс развитию инновационных инициатив на многих факультетах и способствовала созданию различных инфраструктурных инновационных объектов в соответствии с Программой развития МГУ.

На экономическом факультете МГУ к этому времени сформировалось новое научно-образовательное направление по проблемам инновационного развития, в котором приняли участие многие кафедры, по этой тематике проводились многочисленные конференции и Ломоносовские чтения. Перед кафедрой экономики инноваций ([www.ied.econ.msu.ru](http://www.ied.econ.msu.ru)) руководством экономического факультета МГУ имени М.В. Ломоносова была поставлена глобальная задача не только научно-методологической проработки и систематизации знаний в сфере проблем инновационного развития, но и формирования инновационной среды с разнообразными площадками по взаимодействию студентов и всех сотрудников (не только экономического факультета, но и других факультетов МГУ) с представителями реального бизнеса. С этой целью был создан инновационный кластер, включающий кафедру экономики инноваций, Бизнес-клуб МГУ, Студенческий бизнес-инкубатор МГУ, Лабораторию инновационного бизнеса и предпри-



нимательства, Центр развития молодежного предпринимательства, Центр биоэкономики и эко-инноваций и другие структуры.

Ниже представлена инновационная инфраструктура, созданная на экономическом факультете МГУ за рассматриваемый период (рис. 1).

Все сформированные инновационные структуры активно сотрудничают с Научным парком МГУ, Иннопрактикой, Центром трансфера технологий МГУ, Биотехнологическим инкубатором МГУ и другими структурами. Их сетевое взаимодействие представляет собой неформальные механизмы распространения новых идей и способствует возникновению междисциплинарных коопераций, которые сегодня являются наиболее перспективными источниками новых технологий и продуктов.

Таким образом, в этот период были созданы основные элементы инновационной инфраструктуры в МГУ и на экономическом факультете, установлены тесные взаимосвязи со всеми участниками и тем самым заложена основа межфакультетского сотрудничества. Важным итогом совместной деятельности факультетов явилось признание роли экономистов не только в совместном создании и реализации инновационных проектов, но и в необходимости их участия в подготовке кадров нового типа для инновационной экономики.

### Актуализация инновационного образования и подготовка кадров нового типа на основе междисциплинарного подхода

Подготовка кадров нового типа с компетенциями, адекватными требованиям современной инновационной экономики, это новая задача, стоящая перед современной системой образования. Именно в сфере



Рис. 1. Инновационная инфраструктура экономического факультета

инновационного образования и повышения инновационной активности находится ключ перехода России на инновационный путь развития.

Как показывает мировой опыт, для инновационной деятельности требуются специалисты, обладающие особой подготовкой и знаниями, умениями и навыками, обеспечивающими эффективность инновационного процесса. В настоящее время наблюдается недостаток квалифицированных специалистов и менеджеров, владеющих основами предпринимательской деятельности в научно-технической сфере, знаниями и навыками эффективного трансфера и коммерциализации технологий, что существенно сдерживает инновационную активность. Выпускники университетов зачастую не имеют достаточных компетенций для эффективной деятельности в инновационной сфере. Причем следует подчеркнуть, что такими компетенциями должны обладать не только выпускники экономических факультетов, но и выпускники естественнонаучных, юридических, социологических и других факультетов. Поэтому, на наш взгляд, необходимо внедрять в учебные планы различных факультетов учебные дисциплины, формирующие у студентов навыки инновационной деятельности. Эта задача последовательно решалась на экономическом факультете путем создания многоуровневой системы подготовки кадров для инновационной сферы, включая систему дополнительного профессионального образования.

Впервые на экономическом факультете МГУ разработана концепция и методология многоуровневого обучения по новым учебным дисциплинам инновационного профиля для различных факультетов, программ и направлений. Она последовательно реализуется кафедрой экономики инноваций на основе разработанных учебных дисциплин «Основы предпринимательства» (2005), «Экономика инноваций» (2007), «Управление инновационным развитием компаний» (2019), которые предназначены не только для экономистов, но и для студентов других факультетов. Концепция учебного курса «Экономика инноваций» явилась базовой для разработки модифицированных учебных дисциплин: «Экономика, менеджмент и охрана интеллектуальной собственности в наукоемких технологиях» (магистерская программа физического факультета, 2007 г.), «Менеджмент биотехнологий» (межфакультетская магистерская программа, совместно с биологическим факультетом, 2014 г.), «Право и экономика инноваций» (учебный курс в магистерской программе юридического факультета МГУ «Информационные правоотношения в инновационной экономике», 2016 г.). Учебные курсы «Основы предпринимательства» и «Экономика инноваций: создание технологического проекта» представлены на межфакультетских курсах (МФК) и пользуются большой популярностью среди студентов Московского университета. По данным направлениям на экономическом факультете МГУ открыты магистерские программы «Управление развитием бизнеса» и «Инновационный менеджмент». Успешно реализуется программа МБА «Инновации и развитие бизнеса». А учебно-методические комплексы для студентов и преподавателей «Инновационная экономика и техноло-

гическое предпринимательство» (разработаны совместно с РВК, 2015 г.) в настоящее время преподаются более чем в сорока вузах России и СНГ, которые развивают образовательные программы подготовки кадров для инновационной сферы.

### **Развитие межфакультетского взаимодействия между экономическим и юридическим факультетами МГУ**

На основе имеющегося опыта в подготовке кадров для инновационной сферы выстраивалось и взаимодействие экономического и юридического факультетов МГУ. Когда в 2016 г. на юридическом факультете МГУ имени М.В. Ломоносова была открыта новая магистерская программа «Информационные правоотношения в инновационной экономике», кафедра экономики инноваций экономического факультета МГУ с большим удовлетворением восприняла приглашение научного руководителя магистерской программы, профессора кафедры коммерческого права и основ правоуправления В.А. Северина участвовать в реализации учебного плана магистерской программы и представила в качестве обязательной учебную дисциплину «Право и экономика инноваций». Своевременность такого решения была предопределена требованиями к профессиональной подготовке юристов, которые должны иметь твердые знания в области экономики и менеджмента в сфере информационных технологий для инновационной экономики.

В связи с этим **целью** учебной дисциплины «Право и экономика инноваций» является теоретическая подготовка студентов к использованию экономических знаний в сфере правового обеспечения инновационной деятельности в условиях информационного общества и цифровой экономики, необходимости защиты прав граждан, юридических лиц и публично-правовых образований на результаты интеллектуальной деятельности.

Ставя такую цель, мы исходили из того, что для всестороннего понимания процессов превращения инновационных идей в товар нужны не только юридические, но и экономические и другие знания, которые позволяют студентам в полной мере представлять деятельность по коммерциализации объектов интеллектуальной собственности. Следовательно, необходим комплексный подход с привлечением специалистов из смежных областей, то есть обучение должно вестись на базе юридического и экономического образования.

Кроме того, учебная дисциплина «Право и экономика инноваций» структурно выстроена таким образом, чтобы совокупность тем позволила сформировать у студентов систему знаний в сфере экономики инноваций как на макроуровне (теории инновационного процесса, концепции инновационного развития, общая характеристика инноваций и др.), так и на микроуровне (ключевые факторы осуществления инноваций, создание и развитие инновационной компании, выбор инновационной стратегии) в рамках действующего правового поля.

Какие же ключевые задачи и проблемы ставятся и решаются в данной учебной дисциплине?

**1. Формирование у студентов глубоких познаний в области теории инноваций и инновационного развития в Российской Федерации.** В теме 1 «Введение в теорию инноваций. Основные понятия инновационного развития» рассматриваются базовые концепции теории инноваций, основные понятия инновационного развития. Студенты должны получить ответы на следующие вопросы:

1. *В чем сущность и основные свойства инноваций?*
2. *В чем различие понятий «новшество» и «инновация»?*
3. *Какие модели инновационного процесса существуют, в чем их преимущества и недостатки?*
4. *Какова роль технологического предпринимателя в инновационном процессе?*
5. *Кто такие предприниматели-инноваторы и предприниматели-консерваторы?*
6. *Какие виды инноваций существуют?*
7. *В чем состоит сущность подрывных инноваций и как они влияют на развитие компаний?*

На эти и многие другие вопросы дает ответ давно возникшая и непрерывно развивающаяся **теория инноваций**, представляющая собой совокупность концепций и подходов, объясняющих закономерности инновационного развития.

Студенты должны понимать сущность и основные свойства инноваций, при этом нужно четко осознавать, что идея и изобретение — это очень ценно, но это не инновация! Инновация — это только то новшество или изобретение, которое нашло практическое применение. А из этого положения вытекают свойства инноваций: научно-техническая новизна, производственная применимость, коммерческая реализуемость. Таким образом, инновации — это рыночная категория, и из этого следует вывод, что инновации и предпринимательство неразрывны.

Фундаментальные основы понимания сущности инноваций заложены основоположником теории инноваций, австрийским ученым Й. Шумпетером. Именно Й. Шумпетер ввел в научный оборот категорию «инновации» в 1911 г., ему принадлежат знаменитые слова о том, что на уровне технологии это изобретение, а подключение к этому процессу бизнеса превращает изобретение в инновацию.

В данной теме подробно рассматриваются различные типы и виды инноваций, их *классификация* по различным существенным основаниям, критериям, параметрам. Рассматриваются эпохальные, базисные, улучшающие инновации и их роль в развитии общества, раскрываются современные концепции «подрывных» и «открытых» инноваций. Особо подчеркивается, что вопрос о классификации инноваций носит не только теоретический, но и в значительной мере *практический характер*, как основа управления инновациями.

Важное место в данной теме занимают анализ роли и места России в мировом рынке наукоемкой продукции и стратегические задачи инновационного развития российской экономики до 2030 г. в условиях цифровой экономики. Необходимость подготовки профессиональных кадров, в том числе и в сфере юриспруденции, для инновационной экономики России рассматривается законодательное обеспечение инновационной деятельности в РФ.

**2. Развитие углубленных знаний в области формирования инновационной среды и моделей инновационных процессов в России, необходимых для успешной профессиональной работы по правовому регулированию информационно-коммуникационных отношений и защите информации.** Комплекс данных вопросов раскрывается в теме 2 «Внешняя среда инноваций». Студенты должны получить ответы на следующие вопросы:

1. *Каковы условия формирования эффективных инноваций?*
2. *Что такое внутренняя и внешняя среда инноваций?*
3. *Какова структура национальных инновационных систем (НИС)?*
4. *Как связаны наука, образование и инновации?*
5. *Каковы современные тенденции трансформации предпринимательского сектора НИС в условиях цифровой экономики?*
6. *Что такое инновационная инфраструктура и из каких элементов она состоит?*
7. *Какова роль государства в создании инновационной среды?*

Эффективное развитие и коммерциализация инноваций во многом зависит от внешней среды, благоприятствующей или противодействующей инновационному развитию. Формирование такой инновационной среды лежит в двух взаимосвязанных плоскостях:

1) в создании внешних условий, благоприятствующих инновационному развитию, к которым можно отнести совокупность институтов и организаций в структуре национальных инновационных систем (внешняя среда инноваций);

2) в плоскости наличия у хозяйствующих субъектов необходимой внутренней среды — инновационного потенциала, способного генерировать идеи и осуществлять процесс их коммерциализации по всему инновационному циклу (внутренняя среда инноваций).

Такое сочетание внутренней среды и внешних условий, определяемое как инновационная среда, является основополагающим условием осуществления эффективной инновационной деятельности. Ключевой вопрос данной темы — понятие национальной инновационной системы, которая рассматривается как совокупность институциональных рыночных структур, содействующих развитию инновационной экономики каждой страны.

Национальная инновационная система состоит из двух частей: научно-производственной среды и институциональной среды. С точки зрения юридических аспектов особую значимость приобретает характеристика

институциональной среды, которая обеспечивается деятельностью государства в рамках формирования государственной научно-технологической и инновационной политики.

В рамках изучения данной темы студенты юридического факультета рассматривают комплекс институтов правового, финансового и социального характера и изучают совокупность законодательных актов, норм, правил и ведомственных инструкций, обеспечивающих взаимодействие субъектов инновационной деятельности с другими сегментами национальной экономики.

**3. Расширение системы знаний, позволяющих сознавать значение проводимой в Российской Федерации широкомасштабной реформы законодательства об интеллектуальной собственности и защите информации.** Для понимания процессов коммерциализации результатов научно-исследовательской деятельности весьма существенное значение имеют темы, связанные с интеллектуальной собственностью. В рамках данной темы студенты должны получить ответы на следующие вопросы:

1. Что такое интеллектуальная собственность и зачем ее защищать?
2. Какие виды защиты интеллектуальной собственности существуют?
3. Каковы роль и значение интеллектуальной собственности для компаний?



**Рис. 2. Общая структура национальных инновационных систем**

*Источник: составлено основе материалов лекций Иващенко Н.П. по «Экономике инноваций», 2007–2020 годы*

4. *Что такое служебное произведение и чем отличаются авторы и правообладатели?*

5. *Патент или ноу-хау: что выбрать?*

6. *Какие существуют стратегии управления интеллектуальной собственностью?*

7. *Как осуществляется патентный поиск?*

8. *В чем сущность лицензирования? Что такое трансфер технологий?*

9. *В чем суть реформы законодательства об интеллектуальной собственности и защите информации?*

**Интеллектуальная собственность (ИС)** — совокупность личных нематериальных и материальных прав (интеллектуальные права) на результаты интеллектуальной деятельности, принадлежащих авторам, их наследникам и иным юридическим и физическим лицам согласно закону или договору. Интеллектуальная собственность включает: результаты интеллектуальной деятельности (РИД); приравненные к ним средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана.

**Особенности интеллектуальных прав** заключаются в том, что они ограничены сроком действия, ограничены территорией страны или группы стран, являются исключительными — третьи лица не вправе совершать действия с объектами прав без согласия собственника, носят абсолютный характер — действуют против любого лица, допустившего использование чужой интеллектуальной собственности без разрешения собственника.

Роль и значение интеллектуальной собственности в компании определяется тем, что интеллектуальная собственность является одним из решающих факторов создания стоимости, особенно для инновационных продуктов, приносит значительные экономические выгоды, формирует долгосрочные конкурентные преимущества компании, увеличивает капитализацию компании, защищает бизнес от конкурентов, дает возможность получать лицензионный доход. Правовая охрана интеллектуальной собственности ограничена территорией страны, на которой зарегистрировано право. Важно, чтобы магистранты на практике уяснили специфические понятия и терминологию, которые используются в нормотворческой, правоохранительной и правоприменительной деятельности в сфере правовой охраны интеллектуальной собственности и защиты информации. Такая постановка подчеркивает актуальность комплексной подготовки магистров в данной области для нужд инновационной экономики.

**4. Выработка навыков и способности к осуществлению поиска бизнес-идей и креативного решения проблем в инновационной экономике, выбора бизнес-модели в действующем правовом поле, правовых условий по выведению инновационных продуктов на рынок.** Важное место в учебной дисциплине «Право и экономика инноваций» занимают практические вопро-

сы по поиску бизнес-идей и креативных методов их реализации. Студенты должны получить ответы на следующие вопросы:

1. Как осуществляется выбор и генерация идей?
2. Каким образом создается и развивается инновационный продукт?
3. Как создаются, проверяются и внедряются продуктовые гипотезы?
4. Как происходит прототипирование?
5. Что такое *Product Evolution Canvas (PEC)* и *Product Market fit*?
6. Как использовать эти модели?
7. Как выводить инновационные продукты и услуги на рынок?

После проведенных этапов анализа рынка наступает следующий этап исследования — «генерация идей». Идеи — это основы для создания вашего будущего или улучшения существующего продукта или сервиса. Здесь следует обращать внимание студентов, что «хорошие идеи = конкретные предложения», то есть подчеркивается практическая значимость предложений, которые должны описывать будущее ценностное предложение.

Для генерации идей можно использовать следующий инструментарий, который рассматривается со студентами на практических занятиях:

**«Мозговой штурм»** — популярный вид коллективной генерации идей, в основе которой лежит несколько принципов: никакой критики, поддержание мыслей других участников («Да, и...»), фиксация всех предложенных идей, фокус на выбранной тематике, чем больше идей — тем лучше.

**ТРИЗ** (теория решения изобретательских задач) — «наука о том, как ставить и решать задачи». Была создана Г.С. Альтшуллером (1926–1998), инженером-изобретателем.

**ТОС** (теория ограничений систем) — методология управления системами и проектами, базирующаяся на поиске и управлении ключевым ограничением системы (Э. Голдратт, 1980). Согласно методологии, совершенствуя всего лишь малое количество аспектов системы, можно добиться эффекта, превышающего результат воздействия на всю систему в целом или воздействия всех областей системы поочередно.

Важный аспект в анализе комплекса рассматриваемых вопросов занимают проблемы вывода продукта на рынок. Существует множество способов выведения и продвижения инновационных продуктов. В целом они схожи с теми, которые используются и для неинновационных продуктов. Однако в силу ограничений, которые были описаны выше (невысокий бюджет, отсутствие рынка, низкая осведомленность покупателей, ограниченное количество покупателей и т.п.), в учебном курсе рекомендуются способы, которые учитывают правовые условия по выведению инновационных продуктов на рынок.

**5. Анализ организации деятельности малой группы, созданной для реализации конкретного экономического проекта в действующем правовом поле, презентация инновационного проекта инвесторам.** На заключительном этапе учебного курса важное значение имеет демонстрация получен-



ных навыков по созданию и презентации созданного инновационного проекта инвесторам. Студенты должны ответить на вопросы:

1. *Что такое инвестиционная презентация и чем она отличается от других видов?*
2. *На что инвесторы смотрят при презентации проектов?*
3. *В чем специфика рисков инновационных проектов?*
4. *Как можно оценивать риски и управлять ими?*
5. *Карта рисков инновационного проекта: как составлять и зачем использовать?*
6. *В чем состоят «секреты» успешных выступлений?*

Студенты рассматривают важные вопросы по представлению проекта внешней аудитории. Выделяют несколько форматов презентаций перед инвесторами.

Самый короткий формат — elevator pitch, цель такой презентации привлечь внимание к своему проекту, а также договориться о более продолжительной встрече.

Более продолжительный формат (3–5 минут) — idea pitch, короткая презентация, которая представляет идею проекта.

Еще более расширенная версия (от 5 до 10 минут) — funding pitch, на которой особый акцент делается на финансовых показателях и предложении инвестору.

Также часто можно встретить словосочетание pitch deck, что и означает инвестиционную презентацию.

Если рассматривать презентацию с точки зрения инвестора, то вот ключевые вопросы, ответы на которые он ожидает получить ответ во время презентации проекта:

1. *Какую и чью проблему решают?*
2. *Почему это интересный рынок для инвестора?*
3. *Кто конкуренты? Почему предлагаемое решение лучше?*
4. *Почему именно у этой команды это получится?*
5. *На что ищут деньги?*
6. *Почему инвестору стоит инвестировать в проект?*

Рассматриваются также основные риски, свойственные инновационным проектам: риски НИОКР, технологические риски, производственные риски, управленческие и социальные риски, рыночные риски, риски внешней среды.

Содержание и логика обучения по учебной дисциплине «Право и экономика инноваций» позволит студентам юридического факультета МГУ сформировать критическую оценку различных вариантов экономико-правовых решений на микро- и макроуровне, осуществить разработку и обоснование предложений по их совершенствованию с учетом критериев социально-экономической эффективности, финансовых, правовых и экологических рисков и возможных социально-экономических последствий.

С точки зрения исследовательской направленности данная дисциплина будет содействовать выработке навыков и способности к осуществлению экономико-правовых исследований в области современного права и экономики инноваций.

### **Межфакультетские магистерские программы на новом этапе развития Московского университета**

Магистерская программа «Информационные правоотношения в инновационной экономике», в рамках которой экономическим факультетом читается учебный курс «Право и экономика инноваций», фактически является межфакультетской программой. Программа носит междисциплинарный характер и реализуется силами профессорско-преподавательского состава юридического факультета с участием четырех факультетов (экономический факультет, факультет вычислительной математики и кибернетики, Высшая школа государственного аудита, факультет военного обучения) и Института проблем информационной безопасности МГУ. Дальнейшее развитие и совершенствование данной магистерской программы в числе других межфакультетских магистерских программ имеет большое значение для реализации новой Программы развития МГУ до 2030 года.

Ректор Московского университета В.А. Садовничий, характеризуя новый этап в развитии Московского университета, четко обозначил ключевые тенденции современного этапа развития МГУ, который связан с пониманием того, что вся современная научная работа ведется на **междисциплинарном уровне**, на стыке разных наук, а отсутствие готовых многопрофильных специалистов требует создания новых междисциплинарных образовательных программ. Кроме того, как отмечает ректор, все прорывные научные результаты, которые рождаются на основе фундаментальных наук, должны быть реализованы на практике, и в МГУ это будет осуществляться в строящемся сейчас Инновационном научно-технологическом центре «Воробьевы горы», в том числе и в регионах, в рамках консорциума «Вернадский». Реализация этих идей нашла свое воплощение в формировании **Междисциплинарных научно-образовательных школ**, которые будут объединять ученых различных факультетов, а также в активном продолжении строительства Инновационного научно-технологического центра «Воробьевы горы», в создании консорциума «Вернадский» и многих других проектов.

Отметим, что к настоящему времени в Московском университете сформировано семь Междисциплинарных научно-образовательных школ, куда вошли многие факультеты МГУ. У каждой школы три направления деятельности — научная, образовательная и просветительская. Соответственно перед каждой школой стоят три крупные задачи:

1) объединение (консолидация) ученых различных факультетов МГУ для решения актуальной **научной междисциплинарной проблемы**.

Зачастую возникает проблема разрозненности специалистов в соответствующих областях. Специалисты находятся в разных зданиях университета и часто не знают, чем занимаются другие по схожей тематике;

2) подготовка кадров по междисциплинарным научным проблемам в рамках **межфакультетских магистерских программ**. В настоящее время в МГУ работает уже около сорока межфакультетских магистерских программ. Именно понимание необходимости синтеза науки и образования по междисциплинарным проблемам и дало название школам как научно-образовательным школам (ранее они именовались как научные школы);

3) **просветительская деятельность** по выбранной научной проблематике.

Таким образом, межфакультетское сотрудничество между экономическим и юридическим факультетами играет свою очень важную роль в реализации стратегии развития Московского университета по направлению подготовки кадров по междисциплинарным научным проблемам. За прошедшие годы межфакультетская магистерская программа «Информационные правоотношения в инновационной экономике» показала свою эффективность и имеет большой потенциал для дальнейшего развития.

### Литература

1. Программа «Цифровая экономика Российской Федерации» : утв. распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р. URL: <https://www.garant.ru/products/ipo/prime/doc/71634878/>
2. Альварес С. Как создать продукт, который купят. Метод Lean Customer Development / С. Альварес. Москва : Альпина Паблишер, 2018 ; Как создать продукт, который купят: Метод Lean Customer Development : электронное издание. ООО «Альпина Диджитал». URL: [dasreda.ru](http://dasreda.ru).
3. Альтшуллер Г. Найти идею. Введение в ТРИЗ — теорию решения изобретательских задач / Г. Альтшуллер. М. : Альпина Паблишер, 2017. 404 с.
4. Бланк С. Четыре шага к озарению. Стратегии создания успешных стартапов. 2-е изд. / С. Бланк. Москва : Альпина Паблишер, 2017. 600 с.
5. Бланк С. Стартап: Настольная книга основателя. 5-е изд. / С. Бланк, Б. Дорф. Москва : Альпина Паблишер, 2019. 624 с.
6. Иващенко Н.П. Трансформация управленческого образования в условиях цифровой экономики / Н.П. Иващенко // Трансформация бизнес-моделей в условиях цифровой экономики : сборник материалов научно-практической конференции. Москва : Экономический факультет МГУ имени М.В. Ломоносова, 2018. 96 с.
7. Иващенко Н.П. Университеты национальной технологической инициативы как инструмент формирования эффективной науки и экономики знаний в России / Н.П. Иващенко, Е.Б. Кузнецов, А.А. Энговатова // Инновации. 2017. № 1 (219).

8. Инновационная экономика и технологическое предпринимательство : учебное пособие для студента. Санкт-Петербург — Москва : Университет ИТМО, МГУ им. М.В. Ломоносова, Российская венчурная компания, 2019. 165 с.
9. Ицковиц Г. Тройная спираль. Университеты — предприятия — государство. Инновации в действии / Г. Ицковиц ; под ред. А.Ф. Уварова. Томск : Изд-во Томского гос. университета систем управления и радиоэлектроники, 2010. 238 с.
10. Кевин К. Неизбежно. 12 технологических трендов, которые определяют наше будущее / К. Кевин. Москва : Манн, 2017. 460 с.
11. Ким В.Ч. Стратегия голубого океана: Как найти или создать рынок, свободный от других игроков / В.Ч. Ким, Р. Моборн. Москва : Манн, Иванов и Фербер, 2016. 370 с.
12. Котлер Ф. Латеральный маркетинг: технология поиска революционных идей / Ф. Котлер. Москва : Альпина Паблишер, 2010. 170 с.
13. Кристенсен К. Дилемма инноватора. Как из-за новых технологий погибают сильные компании / К. Кристенсен. Москва : Альпина Бизнес Букс, 2019. 240 с.
14. Мур Д. Преодоление пропасти. Как вывести технологический продукт на массовый рынок / Д. Мур. Москва : Litres, 2019. 320 с.
15. Шваб К. Четвертая промышленная революция / К. Шваб. Москва : Эксмо, 2019. 208 с.
16. Шумпетер Й.А. Теория экономического развития. Капитализм, социализм и демократия / Й.А. Шумпетер. Москва : Эксмо, 2007. 861 с.
17. Цифровое производство: методы, экосистемы, технологии : рабочий доклад Департамента Корпоративного обучения Московской школы управления Сколково, октябрь 2017 г. URL: <https://www.skolkovo.ru/news/cifrovoye-proizvodstvo-metody-ekosistemy-tehnologii/>
17. Экономика инноваций : учебно-методическое пособие для программы бакалавров экономического факультета / под ред. Н.П. Иващенко. Москва : Экономический факультет МГУ имени М.В. Ломоносова, 2016. 90 с.
18. Afuah, A. Strategies for Profiting from an Innovation — a dynamic Perspective. Working Paper #9602-06. University of Michigan Business School, 1996. ВП-96-122.pdf (yandex.ru)
19. Granstrand, O. The Economics and Management of Intellectual Property: Towards Intellectual Capitalism. Chapt. 7 Intellectual Property Policies and Strategies. Edward Elgar Publishing, 2000. URL: [https://books.google.ru/books/about/The\\_Economics\\_and\\_Management\\_of\\_Intellectual\\_Property?hl=ru&id=qtrkx8U2cRsC](https://books.google.ru/books/about/The_Economics_and_Management_of_Intellectual_Property?hl=ru&id=qtrkx8U2cRsC)

**Варламова Алла Николаевна,**

профессор кафедры коммерческого права и основ правоведения

Юридического факультета МГУ имени М.В. Ломоносова,

доктор юридических наук

*allavarlamova@mail.ru*

## РЕГУЛИРОВАНИЕ КОНКУРЕНТНЫХ ОТНОШЕНИЙ В ЦИФРОВОЙ ЭКОНОМИКЕ

Рост экономической власти цифровых платформ требует совершенствования антимонопольного регулирования. Данная проблема в настоящее время широко обсуждается в зарубежных странах. В частности, в США проведены расследования в отношении таких компаний, как Google, Apple, Facebook, Amazon. Европейский союз начал разработку антимонопольного законодательства, призванного ограничить доминирование технологических монополий и поддержать конкуренцию.

Российское законодательство о конкуренции также требует изменений. Насколько «пятый антимонопольный пакет» способен решить проблему ограничения российского рынка от незаконного влияния цифровых гигантов, этот вопрос мы попытаемся решить в настоящей статье.

**Ключевые слова:** пятый антимонопольный пакет, конкуренция, цифровые платформы, искусственный интеллект, цифровая экономика, конкурентные стратегии.

**Alla N. Varlamova**

Professor of the Department of Commercial Law and Legal Methods

of the Law Faculty of the Lomonosov Moscow State University

LL.D.

## REGULATION OF COMPETITIVE RELATIONS IN THE DIGITAL ECONOMY

The growth of economic power of digital platforms requires improvement of antimonopoly regulation. This problem is now widely discussed in foreign countries. In particular, in the U.S. there have been investigations of companies such as Google, Apple, Facebook, and Amazon. The European Union has begun developing antitrust legislation designed to limit the dominance of technological monopolies and support competition.

Russian competition law also requires changes. To what extent can the “fifth antimonopoly package” solve the problem of limiting the Russian market from the illegal influence of digital giants. We will try to solve this question in this article.

**Keywords:** fifth antitrust package, competition, digital platforms, artificial intelligence, digital economy, competitive strategies.

Сложно не согласиться с мнением, что «цифровые технологии сегодня оказывают все возрастающее влияние на мировую и национальную экономику, социальную, культурную и политическую сферы жизни государства. Большинство развитых стран реализуют стратегии масштабной цифровизации»<sup>1</sup>.

Данные изменения приводят и к новым методам нарушений правил честной конкурентной борьбы. Критерии рыночной силы, механизмы формирования антиконкурентных соглашений, контроль за экономической концентрацией требуют выработки новых подходов и процедур в части выявления и доказательства.

Однако анализируя вопрос о необходимых изменениях в конкурентном законодательстве, следует принимать во внимание следующее. Появление новых законодательных механизмов не должно заменять глубокого исследования каждого нарушения. Чрезмерная формализацию, появление новых дефиниций в антимонопольном законе, учитывая, что данные дефиниции далеко не всегда имеют совершенно ясные критерии, иногда приводят к тому, что само их наличие дает возможность антимонопольным органам при расследовании избегать глубокого погружения в суть проблемы, ограничиваясь лишь констатацией признаков данных дефиниций. Возможно, поэтому такое нарушение, как установление монополично высоких и монополично низких цен, которые, к примеру, в странах ЕС встречаются достаточно редко именно по причине сложности доказывания, в России занимает значительно большую долю в числе возбужденных антимонопольным органом дел. При доказательстве сговора на торгах антимонопольные органы во многих случаях ограничиваются прежде всего доказательством наличия единой инфраструктуры.

Не хотелось бы, чтобы поправки в Закон о защите конкуренции<sup>2</sup> привели к подобной ситуации в отношении действий цифровых гигантов.

Полагаем, именно беспокойство, что данные поправки могут принести больше вреда, чем пользы, привели к тому, что «пятый антимонопольный пакет» обсуждается уже многие годы и вызвал большое количество возражений. Первую версию «пятого антимонопольного пакета» ФАС России подготовила в марте 2018 г. Данная версия вызвала серьезную критику со стороны Минэкономразвития России. Наибольшее количество сомнений касалось основных дефиниций данного законопроекта — цифровая платформа, сетевые эффекты. Первоначально под цифровой платформой

<sup>1</sup> Алтухов А.В., Кашкин С.Ю. Правовая природа цифровых платформ в российской и зарубежной доктрине // Актуальные проблемы российского права. 2021. № 7. Доступ из СПС «КонсультантПлюс».

<sup>2</sup> Федеральный закон от 26 июля 2006 г. № 135-ФЗ «О защите конкуренции» // СЗ РФ. 2006. № 31 (часть 1). Ст. 3434 (далее — Закон о защите конкуренции).

понимались разнообразные субъекты, оказывающие совершенно разное влияние на рынок, включая электронную биржу, сайты компаний-агрегаторов, сайты интернет-магазинов, сайты туристических фирм, и многое другое.

### Что есть цифровая платформ и сетевые эффекты?

Интересный анализ в части подходов к категории «цифровые платформы» проведен в работе А.В. Алтухова и С.Ю. Кашкина «Правовая природа цифровых платформ в российской и зарубежной доктрине»<sup>3</sup>.

В начале анализа авторы рассматривают в целом такую категорию, как «платформа». «Платформа в самом простом виде определяется как совокупность онлайн-цифровых механизмов, алгоритмы которых обслуживают организацию и структуру экономической и социальной деятельности»<sup>4</sup>.

На основе проведенного анализа различных взглядов авторы работы дают следующее определение цифровой платформы. *Цифровая платформа* — это информационный продукт (рынок), обеспечивающий встречу экономических агентов и связь и взаимодействие между ними, а также место, где они имеют возможность заключать сделки. Интересно то, что информационный продукт авторы приравнивают к категории «рынок».

Как отмечают авторы работы, цифровые платформы применяют бизнес-модель, основанную на всеобъемлющем сборе данных о пользователях. «Они анализируют информацию обо всех видах пользовательской активности: о времени и месте использования (посещения), о записях, комментариях, «лайках», маршрутах перемещения в реальном мире (геолокацию), поисковых запросах, покупках, просмотрах контента и т.д. Собранные данные обрабатываются алгоритмами *искусственного интеллекта* так, чтобы полученная аналитика была оптимизирована для целей маркетинга»<sup>5</sup>.

При определении цифровых платформ используются и несколько иные подходы. Так, А.В. Доценко и А.Ю. Иванов под цифровыми платформами понимают уже не рынок, а продукты — «устройства, программные продукты и информационные сервисы, с помощью которых осуществляется взаимодействие между потребителями и поставщиками разного рода товаров, услуг и информации»<sup>6</sup>.

<sup>3</sup> СПС «КонсультантПлюс».

<sup>4</sup> Kenney M., Zysman J. The Rise of the Platform Economy // Issues in Science and Technology. 2019. Vol. 32. No 3. P. 61, 65.

<sup>5</sup> Алтухов А.В., Кашкин С.Ю. Указ. соч.

<sup>6</sup> Доценко А.В., Иванов А.Ю. Антимонопольное регулирование, цифровые платформы и инновации: дело Google и выработка подходов к защите конкуренции в цифровой среде // Закон. 2016. № 2. С. 37.

В.А. Вайпан совершенно обосновано указывает на необходимость разработки нормативного акта, касающегося специфики контроля за экономической концентрацией при наличии цифровых платформ<sup>7</sup>.

Категории «сетевые эффекты» также в последнее время уделяется значительное внимание в правовой и экономической литературе. Сетевой эффект имеет место в ситуации, когда полезность каждого из потребителей определенной продукции находится в положительной зависимости от количества потребителей этой продукции<sup>8</sup>. В работе «Антимонопольная политика на связанных рынках: теория и практика» под редакцией С.Б. Авдашевой и А.Е. Шаститко<sup>9</sup> упоминаются «двусторонние сетевые эффекты». Полагаем, что, по сути, речь идет именно о прямых и косвенных сетевых эффектах, используемых в проекте пятого антимонопольного пакета.

Первоначально в законопроекте содержалось следующее определение цифровой платформы. *Цифровая платформа* — размещенная в информационно-коммуникационной сети «Интернет» инфраструктура, которая используется для организации и обеспечения взаимодействия покупателей. После длительных дебатов для определения цифровой платформы для целей Закона о конкуренции выделен ряд признаков.

Владение программой (инфраструктурой), которая используется для заключения онлайн-сделок продавцов и покупателей; доля на рынке взаимозаменяемых товаров по обеспечению возможности совершения сделок (должна превышать 35%); наличие «сетевых эффектов» и выручка более 400 млн руб. за последний календарный год от деятельности платформы.

*Прямые сетевые эффекты* выражаются в повышении потребительской ценности товара в результате увеличения числа потребителей. *Косвенные сетевые эффекты* выражаются в зависимости потребительской ценности товара для одной группы потребителей от количества потребителей в другой группе (повышении спроса на продукты смежного товарного рынка).

Несомненно, положительным моментом является то, что согласно последней редакции законопроекта под его действие попали исключительно те цифровые платформы, которые используются для совершения онлайн-сделок (*маркетплейсы и агрегаторы*). Что касается «нетранзакционных платформ» — социальных сетей, поисковых систем, и мессенджеров, то они не попадают под регулирование норм пятого антимонопольного пакета.

<sup>7</sup> Вайпан В.А. Основы правового регулирования цифровой экономики // Право и экономика. 2017. № 11. С. 1.

<sup>8</sup> Юсупова Г.Ф., Сухорукова К.А. Границы рынка и особенности конкуренции на рынках услуг Visa и MasterCard: уроки применения антимонопольного законодательства // Современная конкуренция. 2014. № 6. С. 32.

<sup>9</sup> Антимонопольная политика на связанных рынках: теория и практика / под ред. С.Б. Авдашевой, А.Е. Шаститко. М., 2018. С. 249.



Для понимания влияния цифровых платформ на конкурентные отношения рассмотрим несколько знаковых дел с участием «цифровых платформ».

Если российские антимонопольные органы лишь несколько лет назад впервые столкнулись с проблемами рассмотрения споров с участием цифровых платформ<sup>10</sup>, то за рубежом данная практика имеет уже многолетнюю историю.

Для примера возьмем весьма «старое» дело против в компании *Майкрософт*<sup>11</sup>. Несмотря на то что рассматриваемая ситуация произошла много лет назад, на наш взгляд, данное дело демонстрирует различные подходы к проблеме, в том числе со стороны судебных органов.

Как известно, компания Майкрософт — крупнейший в мире производитель программного обеспечения, реализующий текстовые редакторы (MS Word), программы для работы с таблицами (MS Excel), программы для презентаций (MS Power Point), для работы с электронной почтой (MS Outlook) и базами данных (MS Access).

В 1991–1994 гг. Федеральная торговая комиссия США и Департамент юстиции США проводят антимонопольные расследования в отношении Майкрософт. Было выявлено, что компания с целью увеличения своего присутствия на ряде товарных рынков бесплатно предоставляла свое программное обеспечение производителям процессоров, а также вносило в лицензионные соглашения ряд требований, приводящих к обязательному приобретению связанных продуктов.

В результате проведенного расследования 15 июля 1995 г. было заключено мировое соглашение между Майкрософт и Федеральной торговой комиссией США, основными условиями которого являлись следующие:

- Майкрософт прекращает бесплатное предоставление своего программного обеспечения (ПО) производителям процессоров;
- Майкрософт обязуется не заключать лицензионных соглашений, обязывающих другую сторону приобретать лицензию на иные связанные продукты Майкрософт.

Однако мировое соглашение со стороны Майкрософт было нарушено в 1995 г., когда Майкрософт потребовал от продавцов процессоров установки браузера Internet Explorer в качестве условия, необходимого для продления им лицензии на ОС Windows95. Данное действие привело к снижению доли Netscape Communications Corporation (производитель браузера Netscape Navigator) на рынке браузеров с 70 до 60%. 20 октября 1997 г. Департамент юстиции США постановил, что Майкрософт нарушил мировое соглашение 1995 г., поскольку навязывание

<sup>10</sup> Первое громкое дело — Яндекс против Гугл.

<sup>11</sup> Имеется несколько антимонопольных дел против компании Майкрософт. Мы рассмотрим лишь дело, которое могло привести к принудительному разделению компании.

продавцам компьютеров условия о предустановке Internet Explorer на устройства с ОС Windows95 (которые являются самостоятельными продуктами) давало Майкрософт необоснованное преимущество перед Netscape Communications Corporation. Судебные разбирательства в нескольких инстанциях привели к весьма противоречивым судебным решениям.

В июне 1998 г. Департамент юстиции США подал иск в окружной суд округа Колумбия против Майкрософт, к которому присоединились Генеральные прокуроры 20 штатов и округа Колумбия. Суть иска: Майкрософт планомерно включал в свою ОС Windows программные продукты, которые ранее позиционировал *как отдельные*. Браузер Internet Explorer был интегрирован в ОС Windows для того, чтобы выдвинуть с рынка конкурента — производителя браузера Netscape. Мотивом стали опасения Майкрософт, что Netscape ослабит рыночную власть Майкрософт, поскольку браузеры Netscape совместимы с различными ОС. Таким образом, бесплатное распространение браузера, предустановленного в ОС Windows, было попыткой выиграть войну браузеров и укрепить монополию Майкрософт.

В результате рассмотрения дела были судом сделаны следующие выводы:

1. Продуктовые границы рынка для данного случая — *рынок операционных систем* для персональных компьютеров, работающих на Intel. Именно данной позиции придерживались и истцы.

Майкрософт придерживался иной позиции. По мнению компании, продуктовые границы рынка определены неверно. В качестве продуктовых границ должен был быть определен *рынок платформ для разработки программ и приложений*. Под *платформой* понимается *общий набор кодов и технических данных, существенно упрощающих разработку новых приложений и унифицирующих их, а не операционных систем*. Рыночная сила Майкрософт основана именно на изобилии доступных приложений, а не на преимуществах самой ОС. При этом доля Майкрософт на рынке платформ гораздо меньше, поскольку на нем также присутствуют Netscape Navigator и Sun Java.

2. Майкрософт монополизировал рынок операционных систем, на котором обладает «стабильно большой долей» и препятствует входу конкурентов на смежные рынки.

7 июня 2000 г. окружным судом вынесено решение о мерах ответственности в отношении Майкрософт: разделение на две компании — производителя операционных систем и производителя приложений. При этом топ-менеджеры и акционеры Майкрософт были не вправе сохранить контроль над обоими возникающими правопреемниками одновременно.

Помимо этого, в соответствии с решением на Майкрософт в течение трех лет налагались весьма значительные ограничения, в том числе:

- компания была обязана создать единый прайс-лист для всех покупателей, и цена не должна была зависеть от приобретения покупателем иных продуктов Майкрософт;
- компания была не вправе запрещать своим контрагентам использовать продукты своих конкурентов;
- компания была должна поделиться с конкурентами интерфейсом программирования приложений и иной технической информацией в тех же пределах, в каких она распространяется внутри Майкрософт.

Помимо этого, компания Майкрософт должна была разрешить производителям процессоров вносить существенные изменения в ОС Windows. На компанию налагались ограничения по производству операционных систем, несовместимых для использования с продуктами конкурентов.

Как видно, решение в отношении Майкрософт было весьма жестким и вызывающим, на наш взгляд, серьезные вопросы. Прежде всего, насколько законным было лишать компанию возможности использовать ее конкурентные преимущества? Притом что данные конкурентные преимущества были получены в результате значительных финансовых вложений для достижения технологического лидерства.

Вполне закономерно, что, когда Майкрософт подал апелляцию в Апелляционный суд округа Колумбия, решением этого суда 28 июня 2001 г. предыдущее решение, по сути, было отменено. Главное, что было отменено, *разделение Майкрософт на две компании*. По мнению Апелляционного суда, *связывание Internet Explorer с ОС Windows не нарушает антимонопольных запретов и Майкрософт не пытался монополизировать рынок интернет-браузеров*.

Дело было возвращено в окружной суд.

2 ноября 2001 г. дело прекращено мировым соглашением между штатами США и Майкрософт. Что касается данного соглашения, что можно выделить аспекты и в пользу Майкрософт, и в пользу его конкурентов.

*Что касается положений в пользу Майкрософт:*

- разделение компании не предусматривалось,
- Майкрософт был вправе продолжить расширение функций ОС Windows,
- *отменено общее ограничение на связывание продуктов Майкрософт,*
- Майкрософт не обязан раскрывать конкурентам исходный код технологических продуктов.

Основные положения в пользу конкурентов Майкрософт:

- требование частично раскрыть конкурентам информацию о промежуточном ПО и расширенное толкование промежуточного программного

обеспечения (к нему отнесены браузеры, программы для электронной почты, медиа плееры, мессенджеры);

- требование частично раскрыть протоколы серверов (чтобы сделать взаимодействие между серверами на Windows и не от Майкрософт таким же свободным, как между серверами на Windows и от Майкрософт);
- Майкрософт было запрещено препятствовать производителям процессоров и ПО поддерживать конкурирующее программное обеспечение;
- Майкрософт был обязан предоставить всем желающим производителям процессоров лицензию на 5 лет на равных условиях;
- Майкрософт было запрещено заключать договоры, навязывающие использование только программного обеспечения Майкрософт.

Мы приводим именно это решение, так как, на наш взгляд, оно до настоящего времени является одним из наиболее взвешенных решений в мировой практике в части учета сетевых эффектов. С одной стороны, не ущемляются конкурентные преимущества компании, включая преимущества, которые получены на смежных рынках. При этом предоставляются возможности и для конкурентов «подтянуться за лидером».

Несомненно, есть ряд других антимонопольных дел против компании Майкрософт. Однако, на наш взгляд, именно решение по данному делу является примером взвешенного подхода, учитывающего как интересы «технологического гиганта», так и его конкурентов.

Для сравнения рассмотрим известное в российской практике дело «Яндекс против Гугл». В основе данного дела лежит незаконное, по мнению Яндекса, использование оперативной системы Android, разработанной компанией Гугл. В системе Android, помимо Android Open Source Platform, непосредственно операционной системы, имеется Google Mobile Services (GMS), включающий различные сервисы (Google Maps, Youtube, Gmail), магазин Google Play.

«Яндекс» создали альтернативу GMS — свой магазин Yandex.store. Компания предлагала производителям смартфонов с Android-устройствами предустанавливать их в России вместо сервисов Google. Однако такие предложения не находили поддержки у производителей смартфонов по следующим причинам.

По договору с Гугл магазин приложений Google Play можно было использовать только на следующих условиях:

- обязательной предустановки совместно с магазином приложений Google Play совокупности иных приложений, продуктов, сервисов Гугл;
- обязательной предустановки поисковой системы Гугл по умолчанию;
- обязательного размещения предустанавливаемых совместно с магазином приложений Google Play иных приложений Гугл строго в определенных Гугл местах на экране мобильного устройства;

- соблюдения запрета на предустановку приложений, продуктов, сервисов, разработанных иными хозяйствующими субъектами.

«Яндекс» отмечал, что *связывание Google ОС Android со своими сторонними сервисами* снижало мотивацию пользователей скачивать альтернативные приложения, что также ограничивало конкуренцию.

Изначально дело было возбуждено по такому составу, как недобросовестная конкуренция, однако затем вполне обоснованно было переключено в злоупотребление доминирующим положением.

Основа данного дела в том, как определить границы рассматриваемого товарного рынка. В данном случае антимонопольный орган *магазин приложений рассмотрел как отдельный товар*. Поскольку операционная система iOS, разработанная корпорацией Apple, является закрытой системой и не предоставляется для лицензирования иным производителям мобильных устройств, кроме корпорации Apple, производители мобильных устройств в настоящее время имеют выбор между ОС Android и ОС Windows Phone (доля других операционных систем для мобильных устройств ничтожно мала). При этом переключение на магазин приложений, разработанный под другую операционную систему, невозможно без переключения на другую операционную систему.

Решение ФАС базируется на влиянии косвенных эффектов. Гугл обладает значительной долей на рынке предустановленных магазинов для ОС Android. Это *влияние усиливается в связи с правами на ОС Android*.

В основе предписания ФАС России — недопустимость реализации связанных товаров в рамках единой конкурентной стратегии. При этом аргументы Гугл о том, что магазин приложений нельзя рассматривать как отдельный товар, а также неправильное определение территориальных границ (без учета иностранных потребителей) не были приняты во внимание. Мировое соглашение для публичного анализа недоступно.

Решение вызывает вопросы. Прежде всего, конечно, спорна сама абсолютизированная невозможность использовать конкурентные преимущества на смежном рынке. При этом вложения в разработку операционной системы и ее конкурентные преимущества, благодаря которым она получила признание потребителей, не принимаются во внимание. Вопрос вызывает и обоснованность выделения магазина приложений без сопутствующих товаров как отдельного товарного рынка.

При этом неоднозначен и положительный эффект для конкуренции в результате принятого решения — именно эффект для конкуренции, а не конкретного конкурента.

*Некоторые мысли о пятом антимонопольном пакете.*

Оценивая необходимость поправок для выявления нарушений на рынках с «цифровыми платформами», следует обратить внимание на ряд аспектов.

Первое. Даже в рамках действующего законодательства антимонопольная служба имеет весьма значительные полномочия для устранения нарушений. Примером этого является дело «Яндекс против Гугл», совсем свежее дело против компании Booking, предупреждение Apple (об альтернативных способах оплаты вне App Store).

Второе. Поправки в Закон о защите конкуренции, на наш взгляд, основаны на использовании слишком широкой категории — цифровой платформы и специфики ее регулирования. Полагаем, что предлагаемые поправки могут привести к тому, что формальные критерии (которые сами по себе вызывают большое количество вопросов) будут положены в основу решений по совершенно разным ситуациям с участием разнотипных цифровых платформ. При этом доказательство правонарушений может быть отодвинуто на второй план.

В качестве примера можно привести еще одно весьма знаковое дело, описанное в статье «Сетевые эффекты и недобросовестная конкуренция на рынках цифровых платформ: дело Avito против Auto.ru»<sup>12</sup>. Речь идет о продаже подержанных автомобилей, опубликованных первоначально на сайте Avito. В обоснование своих требований Avito отмечало, что за счет скопированных на сайте Avito объявлений формируется платный продукт «История размещения на Auto.ru». По сути, доказывается наличие получения компанией Auto.ru прямых сетевых эффектов путем увеличения числа объявлений продавцов, что делает платформу более привлекательной для всех заинтересованных лиц.

В данном случае ни ФАС, ни суд не квалифицировали данные действия как злоупотребление доминирующим положением, однако при наличии «пятого антимонопольного пакета» речь вполне могла идти о неких сетевых эффектах. Хотя, на наш взгляд, в рассматриваемом случае вполне достаточно действующих норм Закона о защите конкуренции.

3. Несколько слов о такой слабо используемой российским законодателем категории, как *рыночная сила*.

Сама правовая категория «рыночная сила» заимствована из зарубежного законодательства. Именно выявление наличия «рыночной силы» является определяющим для антимонопольных органов США и Западной Европы при доказывании манипулирования ценами.

«Рыночную силу» с правовых позиций вряд ли можно рассматривать как синоним доминирующего положения. Доминирующее положение привязано к доле рынка, рыночная сила основывается на иных критериях и далеко не всегда имеет непосредственную связь с долей субъекта на рынке.

<sup>12</sup> Петров А.В. Сетевые эффекты и недобросовестная конкуренция на рынках цифровых платформ: дело Avito против Auto.ru // Предпринимательское право. 2020. № 4. Доступ из СПС «КонсультантПлюс».

Полагаем, что определение «рыночной силы» должно найти отражение непосредственно в Законе о защите конкуренции. *Именно данное понятие возможно положить в основу регулирования конкуренции применительно к цифровым рынкам. Учет прямых и косвенных сетевых эффектов должен стать основой критериев рыночной силы цифровых платформ.*

### **Литература**

1. Алтухов А.В. Правовая природа цифровых платформ в российской и зарубежной доктрине / А.В. Алтухов, С.Ю. Кашкин // Актуальные проблемы российского права. 2021. № 7.
2. Антимонопольная политика на связанных рынках: теория и практика / под ред. С.Б. Авдашевой, А.Е. Шаститко. Москва, 2018. С. 249.
3. Вайпан В.А. Основы правового регулирования цифровой экономики / В.А. Вайпан // Право и экономика. 2017. № 11. С. 1.
4. Петров А.В. Сетевые эффекты и недобросовестная конкуренция на рынках цифровых платформ: дело Avito против Auto.ru / А.В. Петров // Предпринимательское право. 2020. № 4.
5. Доценко А.В. Антимонопольное регулирование, цифровые платформы и инновации: дело Google и выработка подходов к защите конкуренции в цифровой среде / А.В. Доценко, А.Ю. Иванов // Закон. 2016. № 2. С. 37.
6. Юсупова Г.Ф. Границы рынка и особенности конкуренции на рынках услуг Visa и MasterCard: уроки применения антимонопольного законодательства / Г.Ф. Юсупова, К.А. Сухорукова // Современная конкуренция. 2014. № 6. С. 32.
7. Kenney M. The Rise of the Platform Economy / M. Kenney, J. Zysman // Issues in Science and Technology. 2019. Vol. 32. No 3. P. 61, 65.

**Крылова Наталья Евгеньевна,**

профессор кафедры уголовного права и криминологии  
Юридического факультета МГУ имени М.В. Ломоносова,  
доктор юридических наук  
*nataliakrylova@mail.ru*

## **КРИПТОВАЛЮТА: УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ РЕГУЛИРОВАНИЯ И ОХРАНЫ**

Статья посвящена проблеме уголовно-правовой оценки криптовалюты как предмета и средства совершения преступления. Автор на основе изучения правового регулирования цифровых прав, цифровой валюты и криптовалюты, изменений уголовного законодательства, связанных с введением состава кражи с банковского счета или в отношении электронных денежных средств, гражданско-правовой и уголовно-правовой доктрины, материалов судебной практики по преступлениям, совершаемым с использованием или в отношении криптовалюты, делает выводы о противоречивости и пробельности правового режима цифровых финансовых активов в целом и криптовалюты в частности, о широком распространении использования криптовалюты в качестве средства оплаты преступной деятельности, включая незаконный оборот наркотических средств и психотропных веществ, фальшивомонетничестве, а также средствах легализации денежных средств и иного имущества, полученных преступным путем, о неприменимости существующего понятия хищения к криптовалюте и единичном характере случаев признания судами криптовалюты предметом хищений. Анализируя имеющуюся судебную практику по делам о разбое в отношении криптовалюты, автор статьи считает правильным квалифицировать подобные случаи как вымогательство, а не разбой.

**Ключевые слова:** уголовный закон, состав преступления, цифровые финансовые активы, цифровой рубль, цифровая валюта, криптовалюта, формы хищения, предмет хищения, хищение с банковского счета или в отношении электронных денежных средств.

**Natalia E. Krylova**

Professor of the Department of Criminal Law and Criminology  
of the Faculty of Law of the Lomonosov Moscow State University  
LL.D.

## **CRYPTOCURRENCY: CRIMINAL LAW ASPECTS OF REGULATION AND PROTECTION**

The article is devoted to the problem of criminal law assessment of cryptocurrency as an object and means of committing a crime. The author on the basis of the study of the legal regulation of digital rights, digital currency and cryptocurrency; changes in criminal law related to the introduction of the composition of theft from a bank account or with respect to electronic funds; civil and criminal law doctrine; materials of judicial practice on crimes committed with or in respect of cryptocurrency, concludes about the inconsistency and gaps in the legal regime of digital financial assets in general and cryptocurrency in particular; widespread use of theft



in relation to cryptocurrency. Analyzing the available judicial practice on cases of robbery of cryptocurrency, the author of the article considers it correct to qualify such cases as extortion, not robbery.

**Keywords:** criminal law, corpus delicti, digital financial assets, digital ruble, digital currency, cryptocurrency, forms of theft, subject of theft, theft from a bank account or in relation to electronic money.

С принятием Федерального закона от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»<sup>1</sup> (далее — Закон о цифровых финансовых активах), введенного в действие с января 2021 г., ряд правовых проблем, связанных с регламентацией цифровых прав и цифровой валюты, получил свое решение.

В соответствии с указанным Законом **цифровые права**, представляющие собой *цифровые финансовые активы*, включают денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, права участия в капитале непубличного акционерного общества, право требовать передачи эмиссионных ценных бумаг, которые предусмотрены решением о выпуске цифровых финансовых активов в порядке, установленном данным Законом, выпуск, учет и обращение которых возможны только путем внесения (изменения) записей в информационную систему на основе распределенного реестра, а также в иные информационные системы (п. 2 ст. 1 ФЗ «О цифровых финансовых активах»).

В свою очередь, **цифровая валюта**, понятие которой важно для нашего исследования, определена как *совокупность электронных данных* (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам (п. 3 ст. 1 ФЗ «О цифровых финансовых активах»).

Таким образом, в соответствии с рассматриваемым Законом основными положениями, на которых базируется регулирование цифровой валюты, являются следующие: 1) цифровая валюта — это совокупность электронных данных; 2) она не является денежной единицей какого-либо

<sup>1</sup> СЗ РФ. 2020. № 31 (часть I). Ст. 5018.

государства, международной денежной единицей или расчетной единицей; 3) может выступать в качестве средства платежа или инвестиции; 4) по отношению к обладателю цифровой валюты отсутствует обязанное лицо.

Следует также отметить, что законодатель не относит *цифровую валюту* к цифровым финансовым активам, хотя в первоначальном проекте Закона о цифровых финансовых активах она к ним относилась. Опираясь на вышеприведенные законодательные определения, установить соотношение цифровых финансовых активов и цифровой валюты, в принципе, невозможно. Это связано с тем, что в обсуждаемом Законе содержание данных терминов раскрывается с использованием несопоставимых выражений: цифровые финансовые активы определены через выражение «цифровые права», а цифровая валюта — через выражение «электронные данные», «цифровой код» и т.д.

Однако цифровые права фиксируются в соответствующей информационной системе также посредством цифрового кода и с технической точки зрения могут быть определены как совокупность электронных данных, но эта внешняя сторона не отражает сущность цифровых прав как правового феномена. В равной степени сущность цифровой валюты не отражает выражение «совокупность электронных данных», поскольку совокупность таких данных никак не может выступать средством платежа или инвестиции.

Таким образом, юридическая природа цифровой валюты остается неопределенной. Исходя из буквального толкования приведенных положений Закона, *цифровая валюта не является цифровым правом*. Не будучи цифровым правом, цифровая валюта не может, следовательно, рассматриваться и как объект гражданских прав (ст. 128 Гражданского кодекса РФ).

В контексте рассматриваемой проблемы представляет интерес Концепция цифрового рубля, представленная Центральным банком РФ в апреле 2021 г.<sup>2</sup> Согласно Концепции, Банк России в целях дальнейшей цифровизации платежной инфраструктуры считает необходимым введение *цифровой национальной валюты — цифрового рубля*. При этом цифровая валюта Центрального банка РФ должна будет выступать равноценной формой национальной валюты — дополнительно к существующим формам денежных средств — и сможет совместить в себе преимущества наличных и безналичных денег<sup>3</sup>. При предлагаемой схеме цифровой рубль будет выступать *обязательством* Центрального банка РФ, который будет обеспечивать легитимность и надежность создания и использования цифрового рубля. В настоящее время рассматривается модель, при которой в качестве циф-

<sup>2</sup> См.: Информация Банка России от 8 апреля 2021 г. «Банк России представил Концепцию цифрового рубля»; «Концепция цифрового рубля» (подготовлена Банком России) // СПС «КонсультантПлюс».

<sup>3</sup> Цифровой рубль. Доклад для общественных консультаций (октябрь 2020 года) (утв. Банком России) // СПС «КонсультантПлюс».

ровой технологии будет использоваться так называемая гибридная архитектура, то есть комбинация распределенных реестров и централизованных компонентов.

Как мы видим, цифровой рубль следует рассматривать скорее как *вид цифровых прав*, нежели цифровую валюту, которая не может быть денежной единицей какого-либо государства. Специалисты указывают на очевидно противоречивый характер определения правовой природы цифрового рубля (как безналичных денег, иного имущества, имущественных прав, цифровых прав, цифровой валюты центрального банка)<sup>4</sup>.

Нерешенность вопроса о правовой природе цифровой валюты влечет противоречивость ее правового режима. Так, в вышеназванном Законе о цифровых финансовых активах, с одной стороны, установлены основы правового регулирования организации обращения цифровой валюты в Российской Федерации, при этом такая организация определена как «деятельность по оказанию услуг, направленных на обеспечение совершения гражданско-правовых сделок и (или) операций, влекущих за собой переход цифровой валюты от одного обладателя к другому, с использованием объектов российской информационной инфраструктуры» (ч. 3 ст. 14 Закона). Иными словами, предполагаются вполне ясная легитимизация цифровой валюты, рассмотрение ее в качестве объекта гражданских прав и предмета гражданско-правовых соглашений, а также разработка специального законодательства, регулирующего обращение цифровой валюты.

С другой стороны, прямо запрещены такие формы оборота цифровой валюты, как ее использование в качестве оплаты (встречного предоставления) за переданные товары, выполненные работы, оказанные услуги (ч. 5 ст. 14 Закона). Кроме того, запрещено распространение информации о предложении и приеме цифровой валюты как способе оплаты товаров, работ и услуг. Из этого следует, что цифровая валюта по-прежнему существенно ограничена в обороте и во многих случаях не может рассматриваться как легальный финансовый инструмент.

Один из главных вопросов — вопрос судебной защиты цифровой валюты — в Законе о цифровых финансовых активах решен таким образом, что защита требований, следующих из обладания цифровой валютой, возможна лишь при условии, что лица, обладающие цифровой валютой, предварительно сообщили о наличии у них такой валюты и о совершении с ней сделок или операций (ч. 6 ст. 14 Закона). Порядок информирования государства о наличии цифровой валюты у конкретного лица и совершении им сделок с ней предполагается закрепить в законодательстве Российской Федерации о налогах и сборах (Налоговом кодексе РФ).

<sup>4</sup> См., напр.: Габов А.В. Цифровой рубль Центрального банка как объект гражданских прав // Актуальные проблемы российского права. 2021. № 4. С. 55–65.

Следует иметь в виду, что понятия «цифровая валюта» и «криптовалюта» не тождественны, хотя многими авторами криптовалюта рассматривается как вид цифровой валюты. Главным их отличием является то, что криптовалюта — всегда децентрализованная виртуальная валюта. Это означает отсутствие в сети единого управляющего центра (администратора), который бы обрабатывал информацию о транзакциях, балансе кошельков владельцев криптовалюты, иную значимую информацию, а также отсутствие субъекта, который осуществлял бы контрольно-надзорные функции<sup>5</sup>.

Закон о цифровых финансовых активах, как было отмечено, крайне противоречиво и весьма ограниченно регулирует правовой режим цифровой валюты, а *криптовалюту не упоминает вовсе*.

В отсутствие внятной законодательной позиции относительно криптовалюты вопрос о ее правовой природе стал предметом активных дискуссий среди представителей наук цивилистического направления. В специальной литературе обсуждается вопрос о том, является ли криптовалюта цифровым финансовым активом и если является, то *можно ли отнести указанный актив к имуществу либо его природа носит обязательственный характер*<sup>6</sup>. При этом отмечается, что «без ответа на указанные вопросы невозможно не только дальнейшее качественное регулирование криптовалюты, но и создание позитивных предпосылок для всего развития современной цифровой экономики в Российской Федерации»<sup>7</sup>.

Ряд ученых-цивилистов предлагают относить криптовалюту к «бестелесным вещам». Так, по мнению Е.Н. Абрамовой, криптовалюта представляет собой *«квази-вещь» («вещеподобный цифровой объект»)*, хотя и лишенную вещественного признака, которую необходимо относить к собственности в широком смысле слова и распространить на нее правовой режим вещей, применяя аналогию закона и права<sup>8</sup>.

А.В. Саженов, рассматривая вопрос об отнесении криптовалюты к имущественным правам, отмечает, что «криптовалюты сами по себе правами не являются и не удостоверяют никакого права, их рассмотрение в качестве имущественных прав сложно себе представить»<sup>9</sup>.

<sup>5</sup> См. об этом подробнее: Рубцова А.С. Криптовалюты: предмет и средство совершения преступления // Вестник Университета имени О.Е. Кутафина (МГЮА). 2018. № 12. С. 175 и далее.

<sup>6</sup> Фролов И.В. Криптовалюта как цифровой финансовый актив в российской юрисдикции: к вопросу о вещной или обязательственной природе // Право и экономика. 2019. № 6. С. 5–17.

<sup>7</sup> Там же.

<sup>8</sup> Абрамова Е.Н. Правовая природа криптовалюты. В кн.: Проблемы создания цифровой экосистемы: правовые и экономические аспекты : монография / коллектив авторов ; под ред. д.ю.н., доц. В.А. Вайпана, д.ю.н., проф. М.А. Егоровой; МГУ им. М.В. Ломоносова, Университет имени О.Е. Кутафина (МГЮА), Моск. отделение Ассоциации юристов России, Междунар. союз юристов и экономистов (Франция). М., 2021. Доступ из СПС «Гарант».

<sup>9</sup> Саженов А.В. Криптовалюты: дематериализация категории вещей в гражданском праве // Закон. 2018. № 9. С. 109.

Е.Н. Абрамова, исследуя данную проблему, приходит к выводу, согласно которому «...криптовалюта по своей сущности не является сама и не содержит в себе обязательственного права, а поэтому не может быть квалифицирована как имущественное право, в том числе цифровое право. Криптовалюта является совершенно иной конструкцией, порождающей вступление ее владельца в комплекс гражданских правоотношений, ни одно из которых не подразумевает реализацию права требования. Указанный комплекс включает абсолютные правоотношения по поводу обладания криптовалютой, относительные правоотношения по поводу заключения с ней различных гражданско-правовых сделок и распоряжения ею, а также организационные правоотношения, связанные с возможностью подтверждения ее существования исключительно по правилам информационной системы путем создания записей в зашифрованном двоичном коде в децентрализованной системе блокчейн»<sup>10</sup>.

Таким образом, вопрос о правовой природе криптовалюты остается нерешенным.

В *сфере уголовного права* возникает множество вопросов, связанных с криптовалютой: должно ли государство охранять отношения по поводу обладания криптовалютой уголовно-правовыми средствами? Можно ли положения Закона о цифровых финансовых активах относительно судебной защиты цифровой валюты распространить на уголовно-правовую защиту криптовалюты — с соблюдением требования об информировании государства о наличии криптовалюты у ее обладателя? В конкретных составах преступлений является ли она предметом или средством их совершения (например, при легализации имущества, приобретенного преступным путем)? Является ли криптовалюта предметом преступлений против собственности, в частности хищений? Если криптовалюта рассматривается как предмет хищения, то в каких формах может происходить посягательство на нее? Как определить размер имущественного ущерба, причиненного владельцу криптовалюты?

В судебной практике криптовалюта чаще всего фигурирует по уголовным делам *о незаконном обороте наркотиков*<sup>11</sup>. Лица, желающие приобрести наркотические средства или психотропные вещества, предварительно

<sup>10</sup> Абрамова Е.Н. Правовая природа криптовалюты. В кн.: Проблемы создания цифровой экосистемы: правовые и экономические аспекты : монография / коллектив авторов ; под ред. д.ю.н., доц. В.А. Вайпана, д.ю.н., проф. М.А. Егоровой ; МГУ им. М.В. Ломоносова, Университет имени О.Е. Кутафина (МГЮА), Моск. отделение Ассоциации юристов России, Междунар. союз юристов и экономистов (Франция). М., 2021. Доступ из СПС «Гарант».

<sup>11</sup> См., напр.: приговор Волоколамского городского суда Московской области № 1-198/2020 от 24 ноября 2020 г. в отношении Оуденко Д.А. // URL: <https://sudact.ru> (дата обращения: 01.10.2021) ; приговор Люберецкого городского суда Московской области № 1-803/2020 от 5 ноября 2020 г. в отношении Стегачева И.С. // URL: <https://sudact.ru> (дата обращения: 01.10.2021).

обменивают свои денежные средства на криптовалюту, которую затем используют для приобретения предметов преступления. Кроме того, лица, участвующие в сбыте наркотических средств в качестве наркокурьеров или закладчиков, нередко получают от организаторов преступных групп вознаграждение в криптовалюте — биткоин, лайткоин, эксмо и проч., после чего конвертируют их в безналичные денежные средства. В подобных случаях криптовалюта выступает инструментом оплаты запрещенных к обороту предметов либо оплаты преступной деятельности. Однако посягательство на саму криптовалюту в этих случаях не осуществляется.

В рамках расследования преступлений данной группы следственно-судебные органы так или иначе обращаются к вопросу о *стоимости единицы криптовалюты* и ее выражении в денежном эквиваленте.

Так, согласно приговору Канского районного суда Красноярского края от 26 октября 2020 г. по делу № 1-75/2020 подсудимый за организованный им один тайник с наркотиком получал оплату от 250 руб. и выше, в зависимости от разновидности наркотика и его веса, при этом расчет был криптовалютой «Биткоин», один «Биткоин» составлял больше 200 000 руб.<sup>12</sup>

Вместе с тем квалификационного значения эти выводы суда, как правило, не имеют, поскольку для уголовно-правовой оценки незаконного сбыта наркотических средств и психотропных веществ важен факт оплаты последних как подтверждение возмездности сделки, а не размер такой оплаты.

Свойства криптовалюты как децентрализованной виртуальной валюты, позволяющей сохранять анонимность ее обладателю и в то же время легко ее конвертировать в законное средство платежа — национальную валюту, используются при совершении и других преступлений, в частности, *при приобретении и сбыте фальшивых денежных знаков*.

Например, приговором Псковского городского суда Псковской области за хранение, перевозку в целях сбыта и сбыт поддельных банковских билетов Центрального банка РФ был осужден гражданин Х., который заказал на сайте «HYDRA» фальшивые купюры номиналом по 5000 руб. в количестве 8 штук для последующего осуществления покупок. Как следует из приговора, фальшивые купюры подсудимый «оплатил криптовалютой — биткоин, которую приобрел на специальном сайте, оплатив 16 000 руб. со своей карты ПАО «Сбербанк»<sup>13</sup>.

В приведенном деле, как и по делам о незаконном обороте наркотиков, криптовалюта служит инструментом оплаты предмета преступления. Однако стоимость фальшивых денег и, следовательно, размер деяния, имеющий значение для квалификации этого преступления (см. ч. 2

<sup>12</sup> Приговор Канского районного суда Красноярского края № 1-75/2020 от 26 октября 2020 г. // URL: <https://sudact.ru> (дата обращения: 02.10.2021).

<sup>13</sup> Приговор Псковского городского суда Псковской области № 1-539/2020 от 15 октября 2020 г. // URL: <https://sudact.ru> (дата обращения: 02.10.2021).

ст. 186 УК РФ), будут определяться не стоимостью потраченных на них биткоинов, а *номиналом* поддельных денег: 8 купюр по 5000 руб., всего 40 000 руб. Именно такой подход применяется на практике<sup>14</sup>.

Криптовалюта может использоваться и для *легализации (отмывания) денежных средств или иного имущества, приобретенных преступным путем* (ст. 174, 174<sup>1</sup> УК РФ). Пленум Верховного Суда РФ разъяснил, что предметами этих преступлений «могут выступать в том числе и денежные средства, преобразованные из виртуальных активов (криптовалюты), приобретенных в результате совершения преступления»<sup>15</sup>.

Из приведенного положения следует, что предметом отмывания являются именно *денежные средства, а не криптовалюта*. Такая позиция Пленума Верховного Суда представляется вполне обоснованной. То обстоятельство, что наркотики, оружие, фальшивые деньги обмениваются на криптовалюту, которая затем конвертируется в денежные средства, не означает, что она является предметом отмывания. В силу ее ограниченного оборота, невозможности выступать законным средством платежа, денежной единицей, в силу нецелесообразности использования в качестве средства накопления из-за высокого риска потерь криптовалюта, как правило, не рассматривается преступниками как самостоятельный предмет отмывания. В действительности целью преступников является не придание правомерного вида владению, пользованию и распоряжению криптовалютой, в этом просто нет необходимости, а *маскирование преступного источника происхождения доходов*.

Судебная практика подтверждает правильность подхода, при котором не криптовалюта, а именно преступно полученные денежные средства или иное имущество рассматриваются в качестве предмета отмывания.

Так, Советским районным судом г. Липецка гражданин М. был осужден по совокупности совершенных преступлений, в том числе по п. «а» ч. 4 ст. 174<sup>1</sup> УК РФ. Согласно приговору, действия М. и его соучастников были направлены на сокрытие нелегального источника происхождения денежных средств, полученных от незаконного сбыта наркотиков. При этом, как отметил суд, использование преступниками схемы приобретения цифровых криптовалют, интернет-приложения «Blockchain Wallet», «деятельность которых не регулируется финансовой системой Российской Федерации и не запрещена законодательством Российской Федерации», предоставило М. и указанным неустановленным лицам «возможность владеть, пользоваться и распоряжаться денежными средствами в сумме 59 010 руб. 22 коп.,

<sup>14</sup> См., напр.: Апелляционные определения Московского городского суда от 11 июля 2014 г. № 10-7972, от 25 июня 2015 г. № 10-7579/15.

<sup>15</sup> Постановление Пленума Верховного Суда РФ «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» от 7 июля 2015 г. № 32 (п. 1) // Бюллетень Верховного Суда РФ. 2015. № 9.

добытыми преступным путем, произведя имитацию происхождения преступного дохода из легальных источников, то есть придало правомерный вид владению указанными денежными средствами для дальнейшего их использования и распоряжения»<sup>16</sup>.

Из приведенного судебного решения видно, что, по мнению суда, использование в преступной схеме криптовалюты, не урегулированной, но в то же время не запрещенной государством, позволило преступникам создать видимость легального источника получения соответствующих денежных средств. Суд указал, что подсудимый М. совместно с участниками организованной группы «осуществлял легализацию *денежных средств, полученных от преступной деятельности*, путем приобретения цифровых криптовалют и дальнейшего использования интернет-ресурсов для имитации происхождения преступного дохода из легальных источников» (выделено мной. — Н.К.)<sup>17</sup>. Именно денежные средства и составили предмет преступления.

На практике встречаются дела, по которым суды исключают обвинение в отмытии денежных средств или иного имущества, приобретенных преступным путем, указывая, что использование криптовалюты в личных целях без ее перевода в безналичные денежные средства невозможно.

Например, в приговоре Фокинского районного суда г. Брянска от 23 июля 2020 г. по делу № 1-139/2020 в отношении гражданина Ш. отмечено, что примененный подсудимым способ получения денежных средств (с использованием различных платежных систем, счетов и банковских карт), несмотря на использование банковского счета гражданки, не осведомленной о преступном происхождении денежных средств, «не свидетельствует о наличии состава преступления, предусмотренного ч. 1 ст. 174<sup>1</sup> УК РФ, поскольку конечной целью было получение наличных денежных средств и их трата на личные нужды, так как иным путем, кроме как конвертировать «биткоин» в рубль и осуществить перевод денег через платежный сервис <...> на банковскую карту, обналичить деньги невозможно»<sup>18</sup>. Действительно, в подобных случаях правильно говорить об отсутствии цели отмытия у лиц, совершающих различные операции с криптовалютой и преобразованными из нее денежными средствами.

Более сложным является вопрос о рассмотрении криптовалюты в качестве возможного *предмета хищения*. В соответствии с примечанием 1 к ст. 158 УК РФ хищение представляет собой «изъятие и (или) обращение чужого *имущества* в пользу виновного или других лиц» (выделено мной. — Н.К.). При этом понятием имущества, которое является гражданско-пра-

<sup>16</sup> Приговор Советского районного суда г. Липецка № 1-259/2020 от 29 июля 2020 г. в отношении Марченко А.Е. // URL: <https://sudact.ru> (дата обращения: 02.10.2021).

<sup>17</sup> Там же.

<sup>18</sup> Приговор Фокинского районного суда г. Брянска № 1-139/2020 от 23 июля 2020 г. // URL: <https://sudact.ru> (дата обращения: 03.10.2021).



вовым, охватываются предметы, обладающие тремя обязательными признаками — материальным (вещественным), экономическим (обладание конкретной стоимостью) и юридическим (принадлежность другому лицу). Неопределенность правового режима криптовалюты, нерешенность вопроса об ее отнесении к объектам гражданских прав, отсутствие у нее признака материальности не позволяют рассматривать ее в качестве предмета хищения.

Вместе с тем в уголовно-правовой доктрине все чаще высказываются предложения об отнесении криптовалюты к предмету хищений. Поскольку, по мнению этих авторов, криптовалюта обладает всеми необходимыми признаками имущества, за исключением одного — материального<sup>19</sup>, то применение норм об уголовной ответственности за хищения следует распространить и на общественно опасные посягательства на данный цифровой объект. Сложившийся подход, согласно которому имущество, чтобы быть предметом хищения, должно обладать признаком «вещественности», рассматривается как устаревший, не учитывающий уровня цифровизации общества, потребностей цифровой экономики и судебной практики.

Встречается и подход, согласно которому для целей уголовного права криптовалюту достаточно отнести к *иному имуществу*. Так, М.М. Долгиева полагает, что «применительно к уголовно-правовым критериям оценки криптовалюты как предмета, объекта или средства преступления достаточно лишь законодательного закрепления криптовалюты как иного имущества. Это, в свою очередь, означает, что криптовалюта как иное имущество может быть средством совершения преступления, например легализации (отмывания) денежных средств; может быть предметом преступления о различных хищениях; криптовалюта может являться объектом киберпреступлений»<sup>20</sup>.

Дополнение в 2018 г. части 3 статьи 158 УК РФ «Кража» пунктом «г», где указано на совершение *кражи с банковского счета, а равно в отношении электронных денежных средств*, было воспринято рядом юристов как прямой отказ законодателя от материального признака имущества в составе кражи и других форм хищения. По мнению этих авторов, постановления Пленума Верховного Суда РФ, в которых дано толкование объективных признаков преступлений против собственности, лишь подтверждают данную позицию законодателя.

Так, П.С. Яни отмечает, что в постановлении от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» Пленум «подтвердил выраженный еще в п. 12 постановления от 27 декабря 2007 г. № 51 взгляд на безналичные денежные средства как на предмет

<sup>19</sup> См., напр.: Немова М.И. Криптовалюта как предмет имущественных преступлений // Закон. 2020. № 8. С. 145–154.

<sup>20</sup> Долгиева М.М. Легализация криптовалюты: судебная практика // Законность. 2021. № 3. С. 50–54.

хищения, а не приобретения права на имущество»<sup>21</sup> (выделено мной. — Н.К.). Как полагает автор, «Пленум вслед за вполне устоявшейся судебной практикой отверг прочно укоренившийся в учении о хищении так называемый физический признак имущества... Замечу, что на заседаниях созданной Верховным Судом рабочей группы по разработке проекта постановления от 30 ноября 2017 г. № 48 большинство профессоров также выступали против распространения состава кражи на противоправное и проч. завладение безналичными средствами. Но были и те — я в том числе, — кто эту позицию как правильно и однозначно ориентирующую суды поддержал».

Далее, переходя к другому вопросу, П.С. Яни замечает: «Поскольку же предметом хищения — на что *прямо указано в законе!* — признаются безналичные, включая электронные, денежные средства, то возникает вопрос о разграничении соответствующих составов: указанного квалифицированного состава кражи и мошенничества с использованием электронных средств платежа» (выделено мной. — Н.К.)<sup>22</sup>.

Однако в уголовном законе как раз **отсутствует** указание на кражу *безналичных денежных средств*. Законодатель сформулировал рассматриваемый признак довольно необычным образом: «с банковского счета, а равно в отношении электронных денежных средств». Ничто не мешало законодателю прямо указать: «кража безналичных денежных средств, в том числе электронных денежных средств», если он посчитал необходимым расширить предмет кражи за счет данных объектов.

На наш взгляд, законодатель ушел от прямого признания этих объектов предметом кражи, указав, скорее, на *место совершения преступления* — «с банковского счета» — по типу состава кражи «из одежды, сумки или другой ручной клади, находившихся при потерпевшем» (п. «г» ч. 2 ст. 158 УК РФ) либо кражи «из нефтепровода, нефтепродуктопровода, газопровода» (п. «б» ч. 3 ст. 158 УК РФ). Указание на такой признак состава преступления, как место его совершения, позволило законодателю решить некоторые правоприменительные проблемы, связанные с определением *момента окончания* подобных хищений и *подследственности*.

По общему правилу, подтвержденному Пленумом Верховного Суда РФ, момент окончания хищений, за исключением разбоя, определяется моментом, когда виновное лицо изъяло имущество и получило реальную возможность пользоваться или распоряжаться имуществом по своему усмотрению (п. 6 постановления Пленума Верховного Суда РФ «О судебной практике по делам о краже, грабеже и разбое» 2002 г.<sup>23</sup>). Однако при краже денежных средств с банковского счета виновное лицо может, не обналичивая деньги, прямо расплачиваться денежными средствами за товары, услуги и т.д.

<sup>21</sup> Яни П.С. Мошенничество с использованием электронных средств платежа. Статья первая // Законность. 2019. № 4. С. 30–35.

<sup>22</sup> Там же.

<sup>23</sup> Бюллетень Верховного Суда РФ. 2003. № 2.

При указании на кражу «с банковского счета» момент окончания преступления должен рассматриваться как более ранний — уже момент списания безналичных денежных средств с банковского счета. Кроме того, в процессе хищения безналичные деньги могут переводиться на счета в различных банках, и тогда возникает проблема определения территориальной подследственности уголовных дел. Именно в таком ключе Пленум Верховного Суда рассматривает эти проблемы в вышеуказанном постановлении по делам о краже, грабеже и разбое 2002 г., отдельно оговаривая как момент и место окончания кражи с банковского счета, так и определение территориальной подсудности уголовных дел по рассматриваемому преступлению (п. 25.2, 25.3 постановления).

Для понимания позиции Пленума относительно предмета кражи с банковского счета имеют значение примеры, приведенные Пленумом в п. 25.1 постановления. В качестве таковых приведены «безналичные расчеты или снятие наличных денежных средств через банкомат», осуществленные «с использованием чужой или поддельной платежной карты». Из примеров видно, что речь идет либо о фактической оплате товаров и услуг посредством безналичных расчетов, либо об обналичивании денежных средств. Но в этих случаях предметом преступления выступает та имущественная масса, которая преобразуется из безналичных денег, в том числе электронных денежных средств.

При исследовании данной проблемы важно ответить на вопрос: почему законодатель, пожелав, как полагают некоторые юристы, отказаться от материального (вещественного) признака имущества, сделал это только в составе кражи, проигнорировав другие формы хищения, например присвоение и растрату, грабеж, разбой, а также близкое к хищению вымогательство? Разве при растрате имущества невозможно, допустим, списание денежных средств организации ее управленцем в счет оплаты приобретаемых лично для себя товаров или услуг? На наш взгляд, законодатель, вводя п. «Г» ч. 3 ст. 158 УК РФ, тем самым решал конкретные правоприменительные задачи, хотя и дал повод для дискуссии относительно расширительного толкования предмета кражи.

Что касается электронных денежных средств, то употребление законодателем формулировки «в отношении электронных денежных средств», в принципе, можно расценить как указание на *предмет преступления*, хотя, как ранее было отмечено, во избежание двусмысленности законодателю было достаточно указать на совершение кражи не «в отношении», а прямо — «кража электронных денежных средств».

Признание электронных денежных средств самостоятельным предметом кражи (что странно с учетом отмеченного выше относительно безналичных денег, но может следовать из законодательной формулировки п. «Г» ч. 3 ст. 158 УК РФ) будет означать существенное расширение предмета кражи и отнесение к такому предмету *имущественных прав*.

В соответствии со ст. 128 ГК РФ безналичные денежные средства, бездокументарные ценные бумаги и цифровые права относятся к имущественным правам<sup>24</sup>. При этом, согласно Федеральному закону «О национальной платежной системе» 2011 г.<sup>25</sup>, электронные денежные средства — *вид безналичных денежных средств*, которые предварительно предоставлены одним лицом другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета, для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа (п. 18 ст. 3).

С учетом понимания электронных денежных средств в гражданском праве, относящем их к имущественным правам, кража, как и мошенничество, становится возможной в двух формах — в форме хищения и в *форме приобретения права на чужое имущество*.

Следует, однако, признать, что любое толкование п. «г» ч. 3 ст. 158 УК РФ не приближает нас к решению проблемы отнесения криптовалюты к предмету кражи, поскольку правовой режим криптовалюты даже в контексте иного имущества, имущественных прав или цифровых прав не определен законодателем. Закон «О цифровых финансовых активах», содержащий определение цифровой валюты, не распространяется на безналичные денежные средства, электронные денежные средства, бездокументарные ценные бумаги, о чем прямо сказано в этом Законе (п. 11 ст. 1). Таким образом, цифровая валюта и различные виды виртуальных валют не могут быть отнесены к безналичным и электронным денежным средствам, а следовательно, п. «г» ч. 3 ст. 158 УК РФ к ним неприменим.

В настоящее время отнесение криптовалюты к предмету хищения следует рассматривать как *аналогию уголовного закона*. Применение аналогии закона или аналогии права, допустимое и оправданное в области гражданского права — при наличии пробелов в законодательном регулировании определенных общественных отношений, обнаруживающих очевидное сходство с отношениями, составляющими предмет гражданско-правового регулирования, *в уголовном праве прямо запрещено*. Данный запрет является составной частью принципа законности (ч. 2 ст. 3 УК РФ).

В юридической литературе тем не менее отмечается, что уголовно-правовая охрана криптовалюты как объекта, обладающего экономической

<sup>24</sup> См.: Абрамова Е.Н. Правовая природа криптовалюты. В кн.: Проблемы создания цифровой экосистемы: правовые и экономические аспекты : монография / коллектив авторов ; под ред. д.ю.н., доц. В.А. Вайпана, д.ю.н., проф. М.А. Егоровой ; МГУ им. М.В. Ломоносова, Университет имени О.Е. Кутафина (МГЮА), Моск. отделение Ассоциации юристов России, Междунар. союз юристов и экономистов (Франция). М., 2021. Доступ из СПС «Гарант».

<sup>25</sup> Федеральный закон от 27 июня 2011 г. № 161-ФЗ (ред. от 02.07.2021) «О национальной платежной системе» // СЗ РФ. 2011. № 27. Ст. 3872.

ценностью, должна осуществляться независимо от правового регулирования ее режима в гражданском законодательстве. Так, М.И. Немова полагает, что «отсутствие регулирования криптовалют не должно означать отсутствия их уголовно-правовой охраны. Действующий Уголовный кодекс РФ не содержит каких-либо формальных ограничений, которые могут предопределить исключение отношений по обороту криптовалют из числа других охраняемых законом общественных отношений»<sup>26</sup>. Таким образом, уголовное право должно реагировать на случаи обманного, общественно опасного, злонамеренного умаления имущественной сферы какого-либо лица, не дожидаясь, когда законодатель урегулирует все вопросы, связанные с выпуском и оборотом криптовалюты в индустриальном законодательстве.

Однако умаление имущественной сферы какого-либо лица помимо его воли может происходить различным образом, и далеко не всегда уголовно-правовые средства к таким случаям могут быть применены. Так, у собственника могут вымогать имущество способом, не указанным в ст. 163 УК РФ «Вымогательство» (например, с использованием угрозы совершить самоубийство, отказаться от заключения брака, лишит жилья, лишит возможности видеться с ребенком после развода и т.д.). Это не означает, что положения о вымогательстве должны применяться к такого рода случаям по аналогии.

По проблеме признания криптовалюты предметом хищения представляет интерес складывающаяся судебная практика. В качестве примера приведем уголовное дело о разбое.

8 апреля 2019 г. приговором Всеволожского городского суда Ленинградской области подсудимые Р.А.АА. и Х. были признаны виновными в разбое и осуждены каждый по п. «б» ч. 4 ст. 162 УК РФ к 10 годам лишения свободы в исправительной колонии строгого режима.

Согласно приговору, 22 марта 2018 года около 00 часов 30 минут в коттеджном поселке Лазурные берега потерпевший и его супруга проснулись от лая собаки. Спустившись на первый этаж, потерпевший на кухне увидел человека в маске, который ударил его прикладом пистолета и приказал сесть. Затем нанес потерпевшему еще два удара кулаком, в котором находился пистолет, в область глаз и губ, после чего связал потерпевшему руки и ноги скотчем. Второй преступник пошел наверх. Когда он спустился, они вдвоем с первым подняли потерпевшего на второй этаж, где посадили в коридоре напротив связанной жены. Старший задал потерпевшему вопрос по поводу пятидесяти, не уточняя чего. Поскольку потерпевший был увлечен криптовалютой, он понял, что речь идет о ней, сказал, что пятидесяти нет и не было, указав, опасаясь за жену

<sup>26</sup> См.: Немова М.И. Криптовалюта как предмет имущественных преступлений // Закон. 2020. № 8. С. 145–154.

и ребенка, что может показать счета. После этого вместе с мужчинами он спустился вниз, где на компьютере, войдя в личный кабинет, показал имеющуюся у него на различных биржах криптовалюту в размере 0,69 и 0,75 биткоина, подтвердив, что готов ее перевести. Мужчина в маске передал ему бумагу с адресом, на который нужно было перевести криптовалюту, а второй стоял позади потерпевшего. От него требовали быстрее переводить, нанесли удары по плечу и в область печени. После этого он на компьютере ввел адрес, указанный на бумаге, и перевел на него имеющиеся у него средства с биржи и «холодного кошелька». По словам потерпевшего, всего нападавших было четверо. Они искали в доме деньги, забрали вещи, затем отвели его наверх, а сами ушли. У двоих нападавших он видел оружие в виде пистолетов, поэтому опасался за свою жизнь, у остальных оружия не было.

Данное судебное решение примечательно тем, что суд *прямо признал криптовалюту предметом разбойного нападения*, поскольку ущерб от преступления описан судом следующим образом: «В результате нападения были похищены 0,671 биткоина, что эквивалентно 310 000 рублей, 0,759 биткоина, что эквивалентно 360 000 рублей, два ноутбука стоимостью более 200 000 рублей и 140 000 рублей, мобильный телефон «Айфон 10», принадлежащий ему (потерпевшему. — Н.К.), мобильный телефон «Айфон 8», принадлежащий жене, мобильный телефон «Айфон си», принадлежащий ребенку, украшения жены, банковские карты «Сбербанк» и «Киви виза», от которых у них спрашивали пин-коды, счетная машинка для денег, а также другое имущество, принадлежащее ему и жене, всего на сумму 1 580 000 рублей».

Учитывая общую сумму ущерба, установленного судом, следует признать, что исключение из этой суммы стоимости криптовалюты непременно повлекло бы изменение объема обвинения и перекалфикацию содеянного на разбой, совершенным лишь в крупном, а не в особо крупном размере (ч. 3 ст. 162 УК РФ).

Для установления объема причиненного потерпевшему имущественного ущерба суд исследовал скриншот «холодного кошелька» с сайта «LEdGER», в соответствии с которым 22 марта 2018 г. в 02 часа 56 минут была произведена транзакция перевода 0,67143272 биткоина, а также скриншот личного кабинета с сайта «BINANCE», в соответствии с которым 22 марта 2018 г. в 04 часа 04 минуты была произведена транзакция перевода 0,75904922 биткоина. Время переводов соответствовало времени совершенного разбойного нападения.

Рублевый эквивалент биткоина был определен судом исходя из «графика» биткоина (BTC) к доллару (USD) за март 2018 г., опубликованного на справочном портале «Калькулятор» в информационно-телекоммуникационной сети «Интернет», при этом 22 марта 2018 г. курс биткоина к доллару, как установил суд, составил 9080 долларов США за 1 биткоин.

Было также учтено, что согласно официальному курсу валют на заданную дату, опубликованному на сайте Банка России в информационно-телекоммуникационной сети «Интернет», 22 марта 2018 г. курс 1 доллара США составлял 57 руб. 49 коп.

Приговор был обжалован стороной защиты, не согласившейся с включением в размер причиненного потерпевшему имущественного ущерба стоимости биткоинов и указавшей, что криптовалюта не является объектом гражданских прав и не может быть предметом преступления, предусмотренного ст. 162 УК РФ. По мнению стороны защиты, не доказан сам факт хищения криптовалюты и принадлежность ее потерпевшему, а кроме того, судом необоснованно признаны доказательствами как иные документы скриншоты «холодных кошельков», представленные потерпевшим в ходе предварительного следствия, которые являются недопустимыми доказательствами.

4 марта 2020 г. Ленинградский областной суд вынес по данному уголовному делу апелляционное определение, которым приговор от 8 апреля 2019 г. *был оставлен без изменения*<sup>27</sup>. Обращает на себя внимание обоснование такого решения. Апелляционная инстанция отметила, что «в силу диспозитивности норм гражданского права в ГК РФ отсутствует закрытый перечень объектов гражданских прав, а потому допустимо максимально широкое его толкование с учетом современных экономических реалий, уровня развития информационных технологий, перспективы принятия законопроекта «О внесении изменений в части первую, вторую и четвертую Гражданского кодекса Российской Федерации», предусматривающего определение базового понятия «цифровое право» в системе объектов гражданских прав».

Давая оценку действиям потерпевшего с криптовалютой, апелляционный суд указал, что «в соответствии со ст. 18 ГК РФ граждане могут иметь имущество на праве собственности, совершать любые не противоречащие закону сделки и участвовать в обязательствах, а также иметь иные имущественные права. Проведение российскими гражданами и организациями операций с использованием криптовалюты не запрещено законами РФ».

Кассационным определением Третьего кассационного суда общей юрисдикции от 1 июля 2021 г. апелляционное определение Ленинградского областного суда от 4 марта 2020 г. было отменено в части, в отмененной части дело передано на новое рассмотрение.

Приведенные судебные решения первой и апелляционной инстанций вызывают множество вопросов, часть из которых уже была рассмотрена в настоящей статье и изложена в апелляционной жалобе стороны защиты. Дополнительно отмечу, что апелляционный суд, подчеркнув, что участники разбойного нападения «сразу» потребовали у потерпевшего перевести

<sup>27</sup> См.: Апелляционное определение Ленинградского областного суда от 4 марта 2020 г. по делу № 22-106/2020 // СПС «КонсультантПлюс».

биткойны на определенные счета, то есть требовали немедленной, а не в будущем, передачи им «имущества», вероятно, тем самым хотел обосновать свою квалификацию содеянного как разбоя, а не вымогательства. Однако в данном случае было упущено из вида то обстоятельство, что преступники *не могли самостоятельно совершить действия по изъятию «имущества» у потерпевшего*, требовалось его обязательное участие. При обычном разбое юридически значимых, встречных действий со стороны потерпевшего не требуется. Из всех форм хищения передача имущества самим потерпевшим возможна лишь в составах мошенничества.

В связи с тем, что изъятие «имущества» в рассматриваемых случаях невозможно без участия потерпевшего, который передает злоумышленникам пароли от личного кабинета, «ключи» от «холодного кошелька», вводит необходимые для перевода криптовалюты данные в информационную систему и т.д., квалификация таких случаев, как разбой, вызывает сомнение. Оценка описанных действий как вымогательства была бы ближе к истине, поскольку вымогательство означает требование, адресованное потерпевшему, о совершении «действий имущественного характера» (ч. 1 ст. 163 УК РФ), каковыми (при их расширительном толковании) можно было бы признать перевод потерпевшим криптовалюты на счета, подконтрольные злоумышленникам.

Помимо уголовных дел о разбое, в судебной практике встречаются дела, возбужденные по статьям о мошенничестве и грабеже<sup>28</sup>. В целом же судебные решения, которыми криптовалюта признавалась бы предметом хищения, носят единичный характер.

Подводя итог нашему исследованию, необходимо отметить, что к настоящему времени криптовалюта вполне «вписалась» в структуру составов преступлений в качестве *средства совершения* преступлений или *платы различных видов преступной деятельности*. Однако в том, что касается хищений, следует признать, что существующие нормы об уголовной ответственности за хищения не могут быть применены к посягательствам на криптовалюту без каких-либо оговорок и применения аналогии уголовного закона. Для уголовно-правовой охраны владельцев криптовалюты перспективным представляется путь формирования *новых составов, отличных от составов хищений, учитывающих правовые и технические аспекты виртуальных валют*.

В любом случае формированию новых уголовно-правовых норм должно предшествовать принятие государством (в лице уполномоченных органов) решения об установлении правовой защиты виртуальных валют, их соответствующая легитимизация. Вместе с тем установление судебной защиты криптовалюты, по логике, должно сопровождаться установлением и опре-

<sup>28</sup> См., напр.: Приговор Октябрьского районного суда г. Тамбова от 15 февраля 2019 г. № 1-134/2019; приговор Кировского районного суда г. Казани от 25 апреля 2019 г. № 1-37/2019.



деленного контроля со стороны государства за выпуском и оборотом криптовалюты, разработкой дополнительных мер безопасности осуществляемых транзакций, определением правил налогообложения и т.д. Но в этом случае криптовалюта утратит свою привлекательность как основанная на анонимности, децентрализации, эффективности с точки зрения обеспечения интересов участников данной платежной системы виртуальная валюта и будет заменена каким-либо новым децентрализованным цифровым объектом.

### Литература

1. Абрамова Е.Н. Правовая природа криптовалюты / Е.Н. Абрамова. В кн.: Проблемы создания цифровой экосистемы: правовые и экономические аспекты : монография / коллектив авторов ; под ред. д.ю.н., доц. В.А. Вайпана, д.ю.н., проф. М.А. Егоровой ; МГУ им. М.В. Ломоносова, Университет имени О.Е. Кутафина (МГЮА), Моск. отделение Ассоциации юристов России, Междунар. союз юристов и экономистов (Франция). Москва, 2021. Доступ из СПС «Гарант».
2. Габов А.В. Цифровой рубль Центрального банка как объект гражданских прав / А.В. Габов // Актуальные проблемы российского права. 2021. № 4. С. 55–65.
3. Долгиева М.М. Легализация криптовалюты: судебная практика / М.М. Долгиева // Законность. 2021. № 3. С. 50–54.
4. Немова М.И. Криптовалюта как предмет имущественных преступлений / М.И. Немова // Закон. 2020. № 8. С. 145–154.
5. Рубцова А.С. Криптовалюты: предмет и средство совершения преступления / А.С. Рубцова // Вестник Университета имени О.Е. Кутафина (МГЮА). 2018. № 12. С. 175 и далее.
6. Саженов А.В. Криптовалюты: дематериализация категории вещей в гражданском праве / А.В. Саженов // Закон. 2018. № 9. С. 109.
7. Фролов И.В. Криптовалюта как цифровой финансовый актив в российской юрисдикции: к вопросу о вещной или обязательственной природе / И.В. Фролов // Право и экономика. 2019. № 6. С. 5–17.
8. Яни П.С. Мошенничество с использованием электронных средств платежа. Статья первая / П.С. Яни // Законность. 2019. № 4. С. 30–35.

**Борисов Михаил Анатольевич,**  
доцент Военного учебного центра  
при МГУ имени М.В. Ломоносова  
*bma\_mv@rambler.ru*

## ПРОБЛЕМЫ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

Целью написания настоящей статьи является совершенствование системы доступа к персональным данным в Российской Федерации в условиях цифровой экономики.

*Модель.* В статье исследованы правоотношения по доступу к персональным данным путем анализа дефиниции нормативных актов и их сравнение с фактической деятельностью организаций.

*Выводы.* Необходимо совершенствование законодательства Российской Федерации в области доступа к персональным данным путем доработки действующих нормативно-правовых актов.

*Ценность.* Материалы, изложенные в статье, помогут совершенствованию действующих нормативных актов, устанавливающих порядок доступа к персональным данным в условиях развития цифровой экономики.

**Ключевые слова:** цифровая экономика, допуск, доступ, персональные данные

**Mikhail A. Borisov**  
Associate Professor of the Military Training Center  
of the Lomonosov Moscow State University

## PROBLEMS OF ACCESS TO PERSONAL DATA IN THE DIGITAL ECONOMY

*Task.* The purpose of this article is to improve the system of access to personal data in the Russian Federation in the digital economy.

*Model.* The article examines the legal relationship on access to personal data by analyzing the definition of normative acts and their comparison with the actual activities of organizations.

*Conclusions.* It is necessary to improve the legislation of the Russian Federation in the field of access to personal data by updating the current regulatory legal acts.

*Value.* The materials presented in the article will help to improve the current regulations that establish the procedure for accessing personal data in the context of the development of the digital economy.

**Keywords:** digital economy, admission, access, personal data

Персональные данные являются одними из самых противоречивых и динамичных разновидностей информации, правовое регулирование которых претерпевает серьезные изменения. Первое упоминание

о «персональных данных» относится к периоду бурного развития вычислительных сетей и появлению такого понятия, как «база данных», когда в 1970 г. в Германии (в ФРГ), в земле Гессен, впервые был принят «Закон о персональных данных». После этого аналогичные законы были приняты в Швеции (в 1973 г.), в Соединенных Штатах (в 1974 г.), в Германии (в 1977 г.) и во Франции (в 1978 г.).

На международном уровне впервые регламентация персональных данных была осуществлена в 1980 г., когда были приняты «Основные положения о защите неприкосновенности частной жизни и международных обменов персональными данными»<sup>1</sup>, в которых были зафиксированы основные принципы работы с ними. Позже на основе вышеуказанного нормативного акта были разработаны Конвенция Совета Европы «О защите прав личности в связи с автоматической обработкой персональных данных» (ETS № 108, г. Страсбург, 28.01.1981) и Руководящие принципы Организации экономического сотрудничества и развития (ОЭСР) «О защите приватности в связи с трансграничной передачей персональных данных», которые существенно повлияли на дальнейшее развитие законодательства о персональных данных во всем мире<sup>2</sup>.

В Российской Федерации правоотношения в области персональных данных регулируют Закон «О персональных данных»<sup>3</sup> и Закон «Об информации, информационных технологиях и о защите информации»<sup>4</sup>. В связи со стремительным развитием «цифровой экономики» и дальнейшим формированием международной нормативной базы, вышеуказанные федеральные законы постоянно подвергаются существенной доработке. По состоянию на октябрь 2021 г. Закон об информации претерпел пятьдесят одну редакцию, а Закон о персональных данных — двадцать шесть. Кроме того, издано более тридцати подзаконных актов, регламентирующих деятельность в области сбора, хранения, уничтожения и обращения с персональными данными граждан Российской Федерации.

Мировое нормотворчество в области обработки персональных данных адаптируется с учетом требований, изложенных в «Генеральном регламенте о защите персональных данных»<sup>5</sup>, который вступил в силу с 25 мая

<sup>1</sup> Защита персональных данных. Опыт правового регулирования / сост. Е.К. Волчинская ; предисл. А.К. Симонов. М. : Галерея, 2001. С. 12–32.

<sup>2</sup> Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. № 8. Изд. 3. М. : Ленанд, 2020. 224 с.

<sup>3</sup> Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. № 31 (часть 1). Ст. 3451.

<sup>4</sup> Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (часть 1). Ст. 3448.

<sup>5</sup> Регламент № 2016/679 Европейского парламента и Совета Европейского Союза «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

2018 г. и расширил сферу действия европейского законодательства, детализировал права субъектов персональных данных, ужесточил обязанности операторов при обработке и защите персональных данных с учетом современных технологий. Обязательства по соблюдению Генерального регламента распространяются не только на юридических лиц, ведущих деятельность на территории двадцати восьми стран Европейского Союза, но и на любые юридические лица вне зависимости от их местонахождения, при условии, что они обрабатывают персональные данные граждан Европейского Союза.

Необходимо отметить, что Генеральный регламент позаимствовал много положений из российского законодательства в области защиты персональных данных, однако соответствие отечественному законодательству не обеспечивает автоматическое соблюдение Генерального регламента, так как ряд процессов и требований введены Генеральным регламентом впервые.

В соответствии с Законом о персональных данных под «персональными данными» понимается «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)», а под «обработкой персональных данных» понимается «любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных». Также к вопросам обработки персональных данных относится и обеспечение «допуска» и «доступа» субъектов к персональным данным. В Законе о персональных данных не выделено самостоятельного понятия «допуск» и закон оперирует только понятием «доступ». Необходимо отметить, что понятие «персональные данные» изначально вводилось исключительно для обозначения цели систематизации информации, обрабатываемой в электронном виде в информационных системах.

Законодательство о персональных данных выделяет трех субъектов персональных данных, которым необходим «допуск» и «доступ» к обрабатываемым персональным данным:

— физическое лицо, персональные данные которого подлежат обработке (ст. 9, 14 Закона о персональных данных);

---

данных)» (принят в г.р. Брюсселе 27.04.2016) // URL: <http://eur-lex.europa.eu> (англ. General Data Protection Regulation, GDPR) (далее по тексту — Генеральный регламент).

— юридическое лицо (оператор), который обрабатывает персональные данные и к которому относятся:

а) оператор персональных данных, находящийся на территории Российской Федерации (ст. 18 Закона о персональных данных);

б) оператор персональных данных, находящийся за пределами территории Российской Федерации (ст. 12 Закона о персональных данных);

в) федеральный орган исполнительной власти — оператор персональных данных (ст. 13 Закона о персональных данных);

— иное лицо — юридическое лицо, осуществляющее обработку персональных данных по поручению оператора персональных данных.

Необходимо отметить, что российское и международное законодательство<sup>6</sup> имеет схожее понятие «оператор персональных данных».

В отношении субъектов, чья обработка персональных данных осуществляется, ч. 3 ст. 14 Закона о персональных данных предусматривает право субъекта на получение информации от оператора о характере обрабатываемых его персональных данных. Указанные права субъект персональных данных может реализовать через своего доверителя (ст. 185 Гражданского кодекса РФ<sup>7</sup>).

С целью своей идентификации (фактически получения «допуска» к своим персональным данным) субъект персональных данных в адрес оператора персональных данных направляет запрос, который содержит:

— сведения о документе, удостоверяющем личность<sup>8</sup>;

— подтверждение участия субъекта в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения) либо сведения, иным образом подтверждающие факт обработки персональных данных оператором;

— подпись субъекта персональных данных. Субъект может выразить свое согласие в виде графической подписи, электронной подписи (как квалифицированной, так и простой), в устной форме с применением биометрического подтверждения голоса<sup>9</sup> и аудиозаписи заявления. С развитием искусственного интеллекта и технологии «NuDetect» получит свое развитие конклюдентная форма подтверждения согласия субъекта.

<sup>6</sup> Opinion 1/2010 On the concepts of “controller” and “processor”. Article 29 Data Protection Working Party. 16 February.

<sup>7</sup> Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ // СЗ РФ. 1994. № 32. Ст. 3301.

<sup>8</sup> Указ Президента РФ от 13 марта 1997 г. № 232 «Об основном документе, удостоверяющем личность гражданина Российской Федерации на территории Российской Федерации» // СЗ РФ. 1997. № 11. Ст. 1301; Постановление Правительства РФ от 8 июля 1997 г. № 828 «Об утверждении Положения о паспорте гражданина Российской Федерации, образца бланка и описания паспорта гражданина Российской Федерации» // СЗ РФ. 1997. № 28. Ст. 3444.

<sup>9</sup> См., напр.: Национальный стандарт РФ. «ГОСТ Р 54412-2011. Информационные технологии. Биометрия. Обучающая программа по биометрии»: утв. Приказом Росстандарта РФ от 21 сентября 2011 г. № 326-ст. М.: Стандартинформ, 2013.

В современный период активно развиваются системы геномной идентификации<sup>10</sup> субъектов персональных данных, которые являются составной частью общей системы развития генетических технологий в Российской Федерации<sup>11</sup>, что соответствует международной тенденции<sup>12</sup>.

В совокупности с положениями Генерального регламента зарубежными специалистами предлагается, в частности, выработать систему инструментов информационного права, когда геномный образ человека будет отнесен к персональным данным<sup>13</sup>. В том же направлении движется и российское законодательство в области персональных данных<sup>14</sup>, предполагающее на первом этапе провести генетическую паспортизацию граждан Российской Федерации.

Решение данного вопроса имеет важное значение для обеспечения безопасности страны. Сбор геномных персональных данных граждан Российской Федерации будет способствовать повышению эффективности борьбы с преступностью, в том числе с терроризмом и экстремизмом, а также будет иметь профилактическое значение и окажет позитивное влияние на криминогенную ситуацию в стране. Создание «Федеральной базы данных геномной информации» (ФБДГИ) граждан Российской Федерации позволит оперативно выявлять и устранять наследственные патологические заболевания, предсказывать эффективность или аллергенность некоторых лекарственных средств, что позволит разрабатывать индивидуальные лекарственные средства, средства против биологического оружия, оперативно локализовывать эпидемии и повышать уровень биологической безопасности России.

<sup>10</sup> Федеральный закон от 3 декабря 2008 г. № 242-ФЗ «О государственной геномной регистрации в Российской Федерации» // СЗ РФ. 2008. № 49. Ст. 5740 ; Постановление Правительства РФ от 11 октября 2011 г. № 828 «Об утверждении Положения о порядке проведения обязательной государственной геномной регистрации лиц, осужденных и отбывающих наказание в виде лишения свободы» // СЗ РФ. 2011. № 42. Ст. 5926 ; Национальный стандарт РФ. «ГОСТ Р ИСО/МЭК 19794-14-2017. Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 14. Данные ДНК» : утв. Приказом Росстандарта РФ от 9 июня 2017 г. № 528-ст. М. : Стандартинформ, 2018.

<sup>11</sup> Указ Президента РФ от 28 ноября 2018 г. № 680 «О развитии генетических технологий в Российской Федерации» (вместе с «Положением о совете по реализации Федеральной научно-технической программы развития генетических технологий на 2019–2027 годы») // СЗ РФ. 2018. № 49 (часть VI). Ст. 7586.

<sup>12</sup> См., напр.: Концепция ответственного обмена геномными данными и данными, связанными со здоровьем человека // URL: <https://www.ga4gh.org/wp-content/uploads/Framework-Russian-translation.pdf>

<sup>13</sup> Бикбулатова Ю.С., Дупан А.С. Использование инструментов информационного права для предотвращения нарушений прав человека в результате проведения исследований его генома: международный опыт // Российская юстиция. 2019. № 9.

<sup>14</sup> Указ Президента РФ от 11 марта 2019 г. № 97 «Об Основах государственной политики Российской Федерации в области обеспечения химической и биологической безопасности на период до 2025 года и дальнейшую перспективу» // СЗ РФ. 2019. № 11. Ст. 1106.

ФБДГИ создавалась в соответствии с принятой во многих странах мира аналогичной системой Combined DNA Index System (CODIS), что гарантирует сопоставимость данных как в России, так и за рубежом в рамках межгосударственного сотрудничества, в том числе по линии Интерпола.

Вместе с тем, как показывает исследование, сбор геномной информации порождает целый ряд морально-этических и других проблем. Так, наличие тех или иных геномных отклонений субъекта может привести к его дискриминации по геномному признаку. Например, запрет на рождение детей некоторыми парами, обязательный отбор и отбраковка предимплантационных эмбрионов и даже аборт по таким медицинским показаниям, работодатели будут отказывать в приеме на работу лицам с сердечно-сосудистыми и другими заболеваниями, будут отбраковывать спортсменов без потенциальных задатков в повышенной выносливости, силы и т.п.

Неправомерное использование геномной информации может спровоцировать повышение доли преступлений в отношении граждан Российской Федерации. Так, утечка информации из ФБДГИ позволит «черным трансплантологам» получить информацию о потенциальном донор-жертве, что может привести к его преждевременной гибели. Хищение геномной информации иностранными спецслужбами позволит создать «генетическое оружие» в отношении многонационального состава граждан Российской Федерации. В 2009 г. в Израиле был проведен эксперимент, когда были сфабрикованы геномные доказательства (кровь и слюна) человека, который на «месте преступления» не был, однако «преступникам» заранее был известен ДНК-профиль данного человека<sup>15</sup>. Следует отметить, что подобная ситуация создает огромные возможности для злоупотребления генетической информацией субъекта, в том числе кражу его генетической идентичности.

Анализ публикаций показывает, что геномная информация является необычной категорией персональных данных, требующей усиленной защиты. Ряд правоведов справедливо предлагает<sup>16</sup> обособить геномные данные в Законе о персональных данных, в Законе об информации и в законодательстве об охране здоровья граждан, отдельно оговорив

<sup>15</sup> Богданова Е.Е. Правовые проблемы и риски генетической революции: генетическая информация и дискриминация // *Lex russica*. 2019. № 6.

<sup>16</sup> См.: Комментарий к Федеральному закону от 3 декабря 2008 г. № 242-ФЗ «О государственной геномной регистрации в Российской Федерации» (постатейный) / отв. ред. Е.Н. Холопова // СПС «КонсультантПлюс», 2016 ; Бикбулатова Ю.С., Дупан А.С. Использование инструментов информационного права для предотвращения нарушений прав человека в результате проведения исследований его генома: международный опыт // *Российская юстиция*. 2019. № 9 и др.

условия предоставления геномной информации членам семьи субъекта персональных данных, а также условия формирования биобанков и системы RWD (англ. «real world data»).

Представляется, что при отнесении геномной информации к персональным данным необходимо учитывать следующие особенности:

а) одним из условий законности обработки собираемой генетической информации является ее целевое ограничение, которое ограничивает свободу исследователя идти на новые открытия и инновации в этой области. Развитие технического прогресса с течением времени будет открывать новые условия и цели обработки геномной информации. Таким образом, принцип «целевого ограничения» геномных персональных данных в данном случае неприменим;

б) по мере развития «цифровой экономики» значение ФБДГИ будет возрастать, соответственно, можно ожидать увеличения объемов и качества собираемой генетической информации. Это, в свою очередь, будет способствовать повышенному интересу разведок иностранных государств и криминальных структур к обрабатываемой в ФБДГИ генетической информации. Степень ущерба, который может быть нанесен Российской Федерации в случае утраты / хищения генетической информации, значителен. Отсюда следует необходимость повышения требований к защите генетической информации, обрабатываемой в ФБДГИ на уровне государства. Существующие сегодня требования к защите персональных данных не обеспечивают адекватных мер защиты, поэтому целесообразно генетическую информацию, содержащуюся в ФБДГИ, отнести к государственной тайне. Причем мероприятия по допуску к государственной тайне, нужно проводить и в отношении должностных лиц, осуществляющих обработку генетической информации в ФБДГИ.

Следующий важный вопрос — это обработка персональных данных. Закон о персональных данных предусматривает два основных условия обработки персональных данных, которые оператор получил от субъекта:

— с письменного согласия субъекта персональных данных (ст. 6, ст. 9 Закона о персональных данных), что фактически является оформленным «допуском»;

— без письменного согласия субъекта персональных данных (в рамках исполнения закона / государственных интересов<sup>17</sup>) (ст. 6, ч. 8 ст. 14 Закона о персональных данных).

<sup>17</sup> Федеральный закон от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // СЗ РФ. 2001. № 33 (часть I). Ст. 3418.



Оператор обязан уведомить уполномоченный орган<sup>18</sup> об обработке персональных данных, за исключением случаев, когда обработка персональных данных осуществляется в рамках трудовых и гражданско-правовых отношений, обработки общедоступной информации, информации, включенной в государственные информационные системы, при обеспечении безопасности и т.п. (ч. 2 ст. 22 Закона о персональных данных). При этом уполномоченный орган обязан проводить периодический государственный контроль и надзор за обработкой персональных данных<sup>19</sup> в случае, если оператор осуществляет:

- обработку персональных данных в государственных информационных системах (ст. 13 Закона о персональных данных);
- сбор биометрических и специальных категорий персональных данных (ст. 10, ст. 11 Закона о персональных данных);
- трансграничную передачу персональных данных на территорию иностранного государства, не обеспечивающего адекватную защиту прав субъектов персональных данных (ст. 12 Закона о персональных данных) или обработку персональных данных по поручению иностранного государственного органа (юридического лица, физического лица), который не зарегистрирован в установленном порядке на территории Российской Федерации.

При обработке персональных данных субъектов оператор решает две основные задачи:

- обеспечение «допуска» и доступа» к персональным данным работников оператора (ст. 18.1 Закона о персональных данных);
- обеспечение «допуска» и «доступа» к персональным данным субъектов персональных данных в соответствии с целями обработки персональных данных (п. 2, 4, 5 ст. 5 Закона о персональных данных).

Механизм обеспечения «допуска» и «доступа» к персональным данным работников оператора Законом о персональных данных не урегулирован

<sup>18</sup> См.: Приказ Минкомсвязи РФ от 14 ноября 2011 г. № 312 «Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных» // Бюллетень нормативных актов федеральных органов исполнительной власти. 2012. № 9 ; Приказ Роскомнадзора РФ от 30 мая 2017 г. № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения» // URL: <http://www.pravo.gov.ru>

<sup>19</sup> Постановление Правительства РФ от 29 июня 2021 г. № 1046 «О федеральном государственном контроле (надзоре) за обработкой персональных данных» (вместе с «Положением о федеральном государственном контроле (надзоре) за обработкой персональных данных») // СЗ РФ. 2021. № 27 (часть III). Ст. 5424.

и фактически отдан на откуп оператору. Так, в ряде локальных нормативных актов<sup>20</sup> под «допуском к обработке персональных данных операторов» понимается «процедура оформления права на доступ к персональным данным», оформляется «допуск» путем «издания приказа о назначении работника на должность, должностной инструкции, предусматривающей обработку персональных данных, заключением обязательства о неразглашении персональных данных». В свою очередь, под «доступом» понимается «возможность обработки персональных данных», при этом «представители сторонних организаций допускаются на основании заключенных договоров, который должен содержать перечень действий (операций) с персональными данными, цели обработки, обязанность лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также перечень требований по защите обрабатываемых персональных данных».

Изучение показывает, что с каждым годом объемы обработки информации постоянно увеличиваются, в том числе растет объем обработки персональных данных. Поэтому все чаще операторы поручают обработку персональных данных третьим лицам, к которым, как правило, относятся различные аутсорсинговые организации (например, ведение бухгалтерии, предоставление вычислительных мощностей и т.п.). В ч. 3 ст. 6 Закона о персональных данных под иными лицами понимается «лицо, осуществляющее обработку персональных данных по поручению оператора». Ключевыми характеристиками такого лица являются:

- наличие самостоятельной правосубъектности (лицо юридически самостоятельное по отношению к оператору);
- обработка данных осуществляется таким лицом в интересах оператора.

В европейском законодательстве связка «оператор» — «иное лицо» рассматривается как «оператор» (англ. «data controller») — «обработчик» (англ. «data processor»)<sup>21</sup>.

Главным отличием оператора от иного лица является распределение ответственности между ними. Так, иное лицо не обязано получать согласие субъекта персональных данных на их обработку. В соответствии с ч. 4, 5 ст. 6 Закона о персональных данных оператор несет ответственность<sup>22</sup> перед субъектом персональных данных за действия иного лица,

<sup>20</sup> См.: Порядок обработки и обеспечения режима защиты персональных данных работников ОАО «РЖД»: утв. Приказом ОАО «РЖД» от 20 июля 2016 г. № 60 «Об обеспечении защиты персональных данных в ОАО «РЖД» // СПС «КонсультантПлюс».

<sup>21</sup> Opinion 1/2010 On the concepts of “controller” and “processor”. Article 29 Data Protection Working Party. 16 February 2010.

<sup>22</sup> См.: ст. 13.11, 13.14, 13.14.1 Кодекса Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // СЗ РФ. 2002. № 1 (часть 1). Ст. 1.

а иное лицо, в свою очередь, перед оператором. Таким образом, субъект персональных данных в силу закона не может предъявить свои требования напрямую иному лицу, такие требования должны быть предъявлены непосредственно оператору.

В данном случае необходимо отметить, что иное лицо по отношению к различным персональным данным может выступать и в роли оператора (например, в отношении своих работников и т.п.). Допуск к обработке персональных данных в интересах оператора «иное лицо» получает в соответствии с поручением оператора. Закон о персональных данных не предусматривает формы и характер такого поручения, которое может представлять собой отдельный договор или отдельные условия в ином договоре. Как правило, заключается агентский договор, договор возмездного оказания услуг и т.п.

В ситуации, когда иное лицо может находиться на территории иностранного государства, законодатель предусмотрел допуск такого лица к персональным данным путем реализации «трансграничной передачи персональных данных». Под «трансграничной передачей персональных данных» понимается отдельный вид обработки таких данных, который заключается в передаче их «на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу» (п. 11 ст. 3 Закона о персональных данных). Таким образом, персональные данные выходят из-под юрисдикции Российской Федерации и попадают под юрисдикцию другого государства.

В практике различают следующие особенности трансграничной передачи персональных данных, которые нужно учитывать субъектам:

— трансграничная передача персональных данных на территорию иностранных государств, являющихся сторонами «Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»<sup>23</sup>, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных<sup>24</sup>. (ч. 1, 2 ст. 12 Закона о персональных данных);

<sup>23</sup> Конвенция о защите физических лиц при автоматизированной обработке персональных данных (заключена в гор. Страсбурге 28 января 1981 г.) (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ № 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15 июня 1999 г.) // СЗ РФ. 2014. № 5. Ст. 419.

<sup>24</sup> Приказ Роскомнадзора РФ от 15 марта 2013 г. № 274 «Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных» // Российская газета. 2013. 26 апреля; Письмо Минкомсвязи РФ от 13 мая 2009 г. № ДС-П11-2502 «Об осуществлении трансграничной передачи персональных данных» // СПС «КонсультантПлюс».

— трансграничная передача персональных данных на территорию иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных (ч. 4 ст. 12 Закона о персональных данных).

Закон о персональных данных не вводит специальных ограничений на трансграничную передачу персональных данных, однако необходимо выполнить ряд условий:

— собираемые оператором персональные данные российских пользователей в обязательном порядке должны сначала «осесть» (локализоваться, зафиксироваться) на территории Российской Федерации, и лишь после этого они могут быть переданы иностранному лицу (оператору, работнику) с соблюдением положений ст. 12 Закона о персональных данных (ч. 5 ст. 18 Закона о персональных данных);

— такое освобождение происходит, если обработка персональных данных осуществляется:

а) для достижения целей, предусмотренных международным договором Российской Федерации или законом, для выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

б) в целях отправления правосудия, исполнения судебного акта;

в) для исполнения полномочий государственными и муниципальными органами;

г) в целях ведения профессиональной деятельности журналиста и / или законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности.

Законом о персональных данных также предусмотрена возможность субъекту относить свои персональные данные к категории общедоступных (ст. 8 Закона о персональных данных). При этом оператор имеет право обрабатывать персональные данные только с письменного согласия субъекта, что является «допуском». Закон о персональных данных не содержит определения «общедоступные категории персональных данных». К источникам образования общедоступных персональных данных относятся различные справочники (телефонные, интернет-адресов и т.п.), интернет-площадки для публикаций информации, порталы «открытых данных» и т.п., которые не предполагают какого-либо ограничения к информации<sup>25</sup>. При этом под общедоступными источниками персональных данных понимаются лишь те, которые создаются по инициативе оператора. К данной категории не относятся информационные

<sup>25</sup> Методические рекомендации по использованию сети Интернет в целях поиска информации о должниках и их имуществе : утв. ФССП РФ 30 ноября 2010 г. № 02-7) // Бюллетень Федеральной службы судебных приставов. 2011. № 1.

системы оператора, которые собирают персональные данные в целях исполнения требований законодательства о раскрытии или опубликовании определенной информации<sup>26</sup> (п. 11 ч. 1 ст. 6 Закона о персональных данных).

На основе вышеизложенного, можно выделить несколько проблем с обеспечением «допуска» и «доступа» субъектов к персональным данным:

1. Характер обрабатываемых персональных данных является весьма разнородным: от «общедоступных» до «генетических», которые по своему характеру наносят различный ущерб в случае их утраты / хищения разведками иностранных государств и криминальными структурами. В соответствии с п. 5 ч. 1 ст. 18.1 Закона о персональных данных оценка ущерба отнесена в ведение оператора, в результате чего разрабатываемые на местах методики оценки<sup>27</sup> носят формальный характер и не отражают прогноз ущерба, который реально может возникнуть. Если для общедоступных персональных данных это не является критичным, то для информации, обрабатываемой в государственных информационных системах, это может привести к значительному ущербу Российской Федерации.

2. Действующее законодательство в области персональных данных урегулирует только вопросы, связанные с технической защитой персональных данных в информационных системах<sup>28</sup>, при этом механизм «допуска» работников (в плане их проверки на предмет действий оформляемого лица, создающих угрозу безопасности Российской Федерации) по аналогии с механизмом допуска к государственной тайне не предусмотрен.

3. Действующее законодательство в области персональных данных не урегулирует механизм «допуска» и «доступа» работников оператора к персональным данным субъекта персональных данных. Порядок «допуска» и «доступа» работников отдан на откуп оператору персональных данных.

4. Развитие «цифровой экономики» Российской Федерации стимулирует развитие различных информационных систем, в том числе

<sup>26</sup> Например, не относятся сведения о ЕГРЮЛ (см. Постановление Президиума Нижегородского областного суда от 6 июля 2016 г. по делу № 44г-49/2016).

<sup>27</sup> См.: Постановление Администрации Тамбовской области от 26 июня 2018 г. № 626 «Об утверждении правил оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных в администрации области» // URL: <http://docs.cntd.ru/document/550130088> и др.

<sup>28</sup> Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // СЗ РФ. 2012. № 45. Ст. 6257; Приказ ФСТЭК РФ от 18 февраля 2013 г. № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.» // Российская газета. 2013. 22 мая.

и государственных информационных систем, в которых накапливаются и обрабатываются персональные данные.

5. В государственных информационных системах обрабатываются персональные данные, объем и важность которых может нанести значительный ущерб безопасности Российской Федерации в случае их утраты / хищения разведками иностранных государств и криминальными структурами<sup>29</sup>.

Существующий пробел целесообразно восполнить путем внесения изменений в следующие нормативные правовые акты:

1) необходимо отнести государственные информационные системы, в том числе и ФБДГИ, в которых обрабатывается информация обо всех гражданах Российской Федерации (лицах без гражданства / иностранных гражданах) к объектам критической информационной инфраструктуры. Для этого п. 8 ст. 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»<sup>30</sup> необходимо изложить в следующей редакции:

«8) субъекты критической информационной инфраструктуры — государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, обработки биометрической и геномной информации, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей, а также государственные информационные системы, в которых централизованно обрабатываются персональные данные всех граждан Российской Федерации».

Это позволит существенно повысить защищенность биометрической и геномной информации, а также персональных данных обрабатываемых в соответствующих государственных информационных системах;

2) необходимо внести следующие дополнения в ст. 5 Закона о государственной тайне:

<sup>29</sup> URL: [https://ics-cert.kaspersky.ru/media/Threats\\_to\\_Biometrics\\_FINAL-RU.pdf](https://ics-cert.kaspersky.ru/media/Threats_to_Biometrics_FINAL-RU.pdf).

<sup>30</sup> Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СЗ РФ. 2017. № 31 (часть 1). Ст. 4736.

«2) сведения в области экономики, науки и техники:

об информации, содержащейся в “Единой информационной системе персональных данных Российской Федерации”<sup>31</sup>;

об информации, содержащейся в “Федеральной базе данных геномной информации”».

Отнесение вышеуказанной информации к государственной тайне будет способствовать тому, что должностные лица, которые будут участвовать в обработке указанной информации, будут допускаться к ней по правилам, предусмотренным к государственной тайне<sup>32</sup>.

Внесение данных правовых норм позволит существенно снизить коррупционную составляющую со стороны должностных лиц, осуществляющих работу с массивами персональных данных граждан Российской Федерации, так как на них будет распространяться соответствующая уголовная<sup>33</sup> и административная<sup>34</sup> ответственность.

### Литература

1. Бикбулатова Ю.С. Использование инструментов информационного права для предотвращения нарушений прав человека в результате проведения исследований его генома: международный опыт / Ю.С. Бикбулатова, А.С. Дупан // Российская юстиция. 2019. № 9.
2. Богданова Е.Е. Правовые проблемы и риски генетической революции: генетическая информация и дискриминация / Е.Е. Богданова // Lex russica. 2019. № 6.
3. Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. № 8. Изд. 3 / М.А. Борисов. Москва : Ленанд, 2020. 224 с.
4. Защита персональных данных. Опыт правового регулирования / составитель Е.К. Волчинская ; предисловие А.К. Симонов. М. : Галерея, 2001. С. 12–32.
5. Комментарий к Федеральному закону от 3 декабря 2008 г. № 242-ФЗ «О государственной геномной регистрации в Российской Федерации» (постатейный) / отв. ред. Е.Н. Холопова // СПС «КонсультантПлюс», 2016.

<sup>31</sup> Постановление Правительства РФ от 30 июня 2018 г. № 772 «Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации» // СЗ РФ. 2018. № 28. Ст. 4234.

<sup>32</sup> Постановление Правительства РФ от 6 февраля 2010 г. № 63 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне» // СЗ РФ. 2010. № 7. Ст. 762.

<sup>33</sup> См.: ст. 275, 276, 283, 283.1, 284 Уголовного кодекса Российской Федерации от 13 июня 1996 № 63-ФЗ // СЗ РФ. 1996. № 25. Ст. 2954.

<sup>34</sup> См.: ч. 7 ст. 13.12, ч. 7 ст. 13.15 Кодекса Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // СЗ РФ. 2002. № 1 (часть 1). Ст. 1.

**Коржова Ирина Вадимовна,**  
ведущий юрисконсульт отдела юридического сопровождения  
деятельности по доверительному управлению  
и корпоративных отношений Юридического департамента  
Акционерного общества «Газпромбанк — Управление активами»  
*irina.korzhova@gazprombank.ru*

## КРИПТОИНВЕСТОРЫ ИЗ РОССИИ: МИФ ИЛИ РЕАЛЬНОСТЬ

В статье рассматриваются проблемные вопросы регулирования, связанные с приобретением российскими инвесторами различных классов криптоактивов.

**Ключевые слова:** инвесторы, квалифицированные инвесторы, неквалифицированные инвесторы, профессиональные участники, криптоактивы, утилитарные цифровые права, цифровые финансовые активы, цифровая валюта, тестирование.

**Irina V. Korzhova**

Leading Legal Counsel of the Legal Support Division trust management activities  
and corporate relations Legal Department  
Joint-stock company Gazprombank -Asset Management

## CRYPTO-INVESTORS FROM RUSSIA: MYTH OR REALITY

The article discusses topical issues related to the ability of crypto investors from Russia to include crypto assets of various classes in their investment portfolio.

**Keywords:** investors, qualified investors, unqualified investors, professional participants, cryptoassets, utilitarian digital rights, digital financial assets, digital currency, testing.

Инвестиционный портфель российского инвестора включает криптоактивы, которые можно разделить на группы по следующим основаниям:

*1. В зависимости от информационной системы, в которой они были выпущены:*

— криптоактивы, выпущенные в российских информационных системах;

— криптоактивы, выпущенные в информационных системах, организованных в соответствии с иностранным правом;



— криптоактивы, выпущенные в нерегулируемых информационных системах<sup>1</sup>.

Криптоактивами, выпущенными в российских информационных системах, являются:

1) утилитарные цифровые права (далее — УЦП), определенные Федеральным законом от 2 августа 2019 г. № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее — Закон о привлечении инвестиций);

2) цифровые финансовые активы (далее — ЦФА) и/или цифровые права, включающие одновременно цифровые финансовые активы и иные цифровые права» (далее — гибридные ЦФА)<sup>2</sup>, определенные Федеральным законом от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее — Закон о ЦФА).

Некоторые особенности содержания, выпуска и обращения криптоактивов, выпущенных в российских информационных системах, представлены в таблице 1.

Применительно к криптоактивам, выпущенным в информационных системах, организованных в соответствии с иностранным правом (далее — иностранные криптоактивы), Банк России в Информационном письме от 19 июля 2021 г. № ИН-06-59/52 «Об отдельных видах финансовых инструментов» (далее — Информационное письмо № ИН-06-59/52) использует терминологию «утилитарные цифровые права, возникшие в инвестиционных платформах, организованных в соответствии с иностранным правом», «цифровые финансовые активы, выпущенные в информационных системах, организованных в соответствии с иностранным правом», «цифровые права, включающие одновременно цифровые финансовые активы и иные цифровые права, выпущенные в информационных системах, организованных в соответствии с иностранным правом».

При этом информация о том, на основании каких признаков оператор обмена ЦФА будет квалифицировать криптоактив на предмет его ответственности признакам того или иного типа иностранного криптоактива, не конкретизируется.

Вместе с тем в различных юрисдикциях приняты свои особенности классификации и определения понятия криптоактивов. Так, например,

<sup>1</sup> Под нерегулируемыми понимаются информационные системы, организация которых не урегулирована законодательством какой-либо юрисдикции.

<sup>2</sup> Далее по тексту статьи гибридные ЦФА не будут упоминаться в качестве самостоятельного вида инвестиционных активов, так как в соответствии с п. 6 ст. 1 Закона о ЦФА выпуск, учет и обращение гибридных ЦФА осуществляются в соответствии с требованиями Закона о ЦФА к выпуску, учету и обращению ЦФА.

Таблица 1

**Особенности содержания, выпуска и обращения криптоактивов,  
выпущенных в российских информационных системах**

Признак/вид	УЦП	ЦФА
<b>1. Удостоверяемые права (требования)</b>	1) право требовать передачи вещи (вещей), исключительных прав на результаты интеллектуальной деятельности; 2) право требовать выполнения работ и (или) оказания услуг	1) денежные требования; 2) возможность осуществления прав по эмиссионным ценным бумагам; 3) права участия в капитале непубличного акционерного общества, 4) право требовать передачи эмиссионных ценных бумаг
<b>2. Особенности выпуска и обращения</b> <b>2.1. Требования к информационной системе</b>	Возникновение, осуществление, распоряжение или ограничение распоряжения УЦП возможны только <i>в инвестиционной платформе<sup>1</sup></i> , соответствующей требованиям <i>Закона о привлечении инвестиций</i>	Выпуск, учет и обращение ЦФА возможны только путем внесения записей в <i>информационную систему, соответствующую требованиям Закона о ЦФА</i>
<b>2.2. Порядок приобретения и отчуждения</b>	Через операторов инвестиционных платформ <sup>2</sup> или через операторов обмена ЦФА <sup>3</sup> (п. 13,14 ст. 8 Закона о привлечении инвестиций).	
<b>2.3. Порядок обмена</b>	Через операторов обмена ЦФА (п. 1 ст. 10 Закона о ЦФА).	

<sup>1</sup> В соответствии с подп. 1 п. 1 Закона о привлечении инвестиций инвестиционная платформа — информационная система в информационно-телекоммуникационной сети «Интернет», используемая для заключения с помощью информационных технологий и технических средств этой информационной системы договоров инвестирования, доступ к которой предоставляется оператором инвестиционной платформы.

<sup>2</sup> По состоянию на 27 августа 2021 г. лишь 2 (две) инвестиционные платформы (Общество с ограниченной ответственностью «Ближкие Горизонты — Инвестиционная платформа», адрес сайта: [www.nhip.ru](http://www.nhip.ru) и Акционерное общество «Регистраторское общество «СТАТУС», адрес сайта: [www.invest.rostatus.ru](http://www.invest.rostatus.ru).) из 41 (сорока одной) включенной в реестр операторов инвестиционной платформы Банка России предоставляют возможность инвестирования путем приобретения УЦП или ЦФА. Данные приведены согласно правилам инвестиционных платформ соответствующих операторов инвестиционных платформ.

<sup>3</sup> Сведения об операторах обмена ЦФА, через которые инвесторы могут совершать сделки с криптоактивами (цифровыми правами) и которые включены в реестр Банка России по состоянию на 27 августа 2021 г., не раскрыты на официальном сайте Банка России.

на Мальте криптоактивы классифицируются в качестве таковых на основании теста финансовых инструментов, разработанного Управлением финансовых услуг Мальты (MFSA)<sup>3</sup>. В Лихтенштейне в Законе TVTG<sup>4</sup> в основе определения токена лежит концепция модели токена как контейнера<sup>5</sup>.

Нормативные акты в Российской Федерации регулируют лишь некоторые особенности обращения ЦФА, выпущенных в информационных системах, организованных в соответствии с иностранным правом (далее — иностранные ЦФА). В частности, любые сделки с иностранными ЦФА могут совершаться только квалифицированными инвесторами через операторов обмена ЦФА, деятельность которых регулируется Законом о ЦФА.

Среди криптоактивов, выпущенных в нерегулируемых информационных системах, наиболее значимыми по ликвидности и капитализации являются криптовалюты<sup>6</sup> (или «цифровые валюты» в терминологии российского законодательства)<sup>7</sup>, под которыми понимаются счетные единицы, которые не удостоверяют никаких прав к эмитенту или прав на какие-либо объекты гражданских прав<sup>8</sup>.

Российское законодательство не регулирует деятельность субъектов, через которые можно приобрести цифровую валюту, но и не запрещает ее покупку через иностранные криптобиржи / криптообменники / иные торговые площадки или напрямую у других участников<sup>9</sup>.

<sup>3</sup> Данный тест используется для квалификации криптоактивов в качестве виртуальных финансовых активов методом исключения, то есть через подтверждение того, что криптоактив не является финансовым инструментом, электронными деньгами или виртуальным токеном (то есть криптоактивом, использование которого ограничено рамками платформы DLT, на которой были выпущены). Подробнее см.: Закон о цифровых финансовых активах Virtual financial assets act 2018 // URL: [www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=12872&l=1](http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=12872&l=1)

<sup>4</sup> Закон о токенах и организациях, предоставляющих услуги на основе доверенных технологий (TVTG) // URL: <https://impuls-liechtenstein.li/en/blockchain/>

<sup>5</sup> Токен, как контейнер, может содержать в себе право на реальный актив (акции, облигации, золото, недвижимость, биржевой товар и др.). Если токен не обеспечен, то он представляет собой «пустой контейнер», существующий в виде цифрового кода, как, например, биткойн. См.: Санникова Л.В., Харитонов Ю.С. Цифровые активы: правовой анализ : монография // 4 Принт. 2020. С. 106–107.

<sup>6</sup> Цифровая валюта (криптовалюта) Bitcoin в сравнении с другими криптоактивами обладает самой высокой рыночной капитализацией, которая по состоянию на 27 августа 2021 г. превышает 63 трлн рублей, по данным сайта CoinMarketCap. URL: <https://coinmarketcap.com/ru/currencies/bitcoin/>

<sup>7</sup> Отдельные нормы, посвященные цифровой валюте, содержатся в Законе о ЦФА (ст. 14 Закона о ЦФА).

<sup>8</sup> Жужжалов М.Б., Толкачев А.Ю. Криптовалюта как имущество — анализ текущего правового статуса // Вестник экономического правосудия Российской Федерации. 2018. № 9.

<sup>9</sup> В соответствии с п. 4 ст. 14 Закона о ЦФА организация выпуска и (или) выпуск, организация обращения цифровой валюты в Российской Федерации будут регулироваться отдельными федеральными законами, которые по настоящее время еще не приняты.

2. *В зависимости от возможности свободного приобретения инвесторами:*
- криптоактивы, которые могут свободно приобретаться «без соблюдения установленных ограничений»;
  - криптоактивы, приобретение которых возможно только квалифицированными инвесторами;
  - криптоактивы, инвестирование в которые возможно только с соблюдением установленных лимитов;
  - криптоактивы, в которые инвестировать не рекомендуется (прямые ограничения или запреты отсутствуют) (далее — *нерекомендованные криптоактивы*).

*Криптоактивы, которые могут свободно приобретаться «без соблюдения установленных ограничений»*

Характерной особенностью данной группы ЦФА являются низкие рыночные риски для инвесторов, связанные с приобретением соответствующих ЦФА. Примером рыночного риска является риск возникновения убытков вследствие неблагоприятного изменения рыночной стоимости финансовых инструментов, а также курсов иностранных валют и процентных ставок.

В соответствии с п. 2 Указания Банка России от 25 ноября 2020 г. № 5635-У<sup>10</sup> (далее — Указание № 5635-У) к низкорискованным относятся ЦФА, которые:

- удостоверяют возможность осуществления прав по включенным в котировальные списки биржи эмиссионным ценным бумагам, за исключением облигаций, или право требовать передачи указанных ценных бумаг;
- удостоверяют возможность осуществления прав по облигациям федерального займа или право требовать передачи указанных облигаций;
- удостоверяют возможность осуществления прав или право требовать передачи облигаций, в случае если их эмитент или лицо, предоставившее обеспечение по облигациям, имеют кредитный рейтинг не ниже уровня, установленного Советом директоров Банка России;

<sup>10</sup> Указание Банка России от 25 ноября 2020 г. № 5635-У «О признаках цифровых финансовых активов, приобретение которых может осуществляться только лицом, являющимся квалифицированным инвестором, о признаках цифровых финансовых активов, приобретение которых лицом, не являющимся квалифицированным инвестором, может осуществляться только в пределах установленной Банком России суммы денежных средств, передаваемых в их оплату, и совокупной стоимости иных цифровых финансовых активов, передаваемых в качестве встречного предоставления, об указанных сумме денежных средств и совокупной стоимости цифровых финансовых активов» (зарегистрировано в Минюсте России 21.12.2020 № 61622).

— включают денежные требования, размер которых эквивалентен стоимости драгоценного металла, наименование и масса которого указаны в решении о выпуске указанных ЦФА;

— кредитный рейтинг ЦФА, включающих денежные требования, не ниже уровня, установленного Советом директоров Банка России.

*Криптоактивы, приобретение которых возможно только квалифицированными инвесторами*

В соответствии с п. 1 Указания № 5635-У признаки соответствующих криптоактивов определены только для ЦФА.

Указанные признаки можно разделить на две группы:

1) признаки, характеризующие особенности прав, которые удостоверяют ЦФА в тех случаях когда:

— ЦФА удостоверяют возможность осуществления прав по эмиссионным ценным бумагам, приобретение которых может быть осуществлено исключительно лицами, являющимися квалифицированными инвесторами, или право требовать передачи указанных ценных бумаг;

— в решении о выпуске ЦФА, включающих денежные требования, не указан срок, в течение которого лицо, выпускающее ЦФА, обязано полностью исполнить обязательство, денежное требование по которому включено в ЦФА;

— получение выплат по ЦФА, включающим денежные требования, поставлено в зависимость от наступления или ненаступления одного или нескольких обстоятельств, предусмотренных абзацем вторым подп. 23 п. 1 ст. 2 Федерального закона от 22 апреля 1996 г. № 39-ФЗ «О рынке ценных бумаг» (далее — Закон о рынке ценных бумаг).

Выделение признаков, отнесенных к первой группе, соответствует объективной потребности защиты неквалифицированных инвесторов, поскольку основано на анализе содержания и порядка реализации прав, которые удостоверяют соответствующие ЦФА;

2) признак (и), предопределенный (ые) видом информационной системы, в том случае, когда ЦФА выпущены в информационных системах, организованных в соответствии с иностранным правом.

Применительно к этой группе лишение неквалифицированного инвестора права приобретать иностранные ЦФА представляется излишним, так как основано исключительно на «национальной принадлежности» информационной системы, в которой они были выпущены, а не на сути активов.

*Криптоактивы, инвестирование в которые возможно только с соблюдением установленных лимитов*

Такие лимиты установлены для некоторых видов ЦФА и УЦП, выпущенных в российских информационных системах.

В отношении ЦФА, непредназначенных только для квалифицированных инвесторов и не относящихся к группе низкорискованных финансовых инструментов, в п. 3 Указания № 5635-У установлено правило, согласно которому неквалифицированные инвесторы могут приобретать такие ЦФА при условии, что сумма денежных средств, передаваемых в их оплату, или совокупная стоимость иных ЦФА, передаваемых в качестве встречного предоставления, не превышает 600 тыс. руб. в течение одного года.

Применительно к криптоактивам, которые приобретаются инвесторами через инвестиционную платформу, действует аналогичное правило. В соответствии с п. 1 ст. 7 Закона о привлечении инвестиций физическое лицо в течение одного календарного года может инвестировать денежные средства с использованием инвестиционных платформ в сумме не более 600 тыс. руб. с учетом инвестирования такого физического лица иными способами<sup>11</sup> в тот же период с использованием нескольких инвестиционных платформ.

Между тем приведенные ограничения не распространяются на инвесторов в статусе юридического лица (применительно к ЦФА<sup>12</sup>) и на инвесторов в статусе индивидуального предпринимателя (применительно к инвестированию через инвестиционные платформы<sup>13</sup>) и по этой причине выглядят мнимыми и не отвечающими потребностям защиты слабых неквалифицированных инвесторов.

Кроме того, возникает вопрос: как специальные субъекты будут отслеживать суммы денежных средств, вложенные инвестором в криптоактивы через других специальных субъектов?

На наш взгляд, ограничения на приобретение криптоактивов неквалифицированными инвесторами эффективнее устанавливать через механизм тестирования, который вводится для некоторых видов финансовых инструментов (необеспеченные сделки, структурные облигации, иностранные ETF, другие) в соответствии с Федеральным законом от 31 июля

<sup>11</sup> В соответствии со ст. 5 Закона о привлечении инвестиций инвестирование с использованием инвестиционной платформы может осуществляться следующими способами:

- 1) путем предоставления займов;
- 2) путем приобретения эмиссионных ценных бумаг;
- 3) путем приобретения утилитарных цифровых прав;
- 4) путем приобретения цифровых финансовых активов.

<sup>12</sup> Пункт 4 Указания № 5635-У.

<sup>13</sup> Пункт 2 ст. 7 Закона о привлечении инвестиций.

2020 г. № 306-ФЗ «О внесении изменений в Федеральный закон «О рынке ценных бумаг» и отдельные законодательные акты Российской Федерации» (далее — Закон № 306-ФЗ) с 1 октября 2021 г., так как тестирование позволяет профессиональным участникам оценить уровень знаний и опыта подопечного им инвестора и предотвратить в случае необходимости неразумные вложения.

### *Нерекомендованные криптоактивы*

В число нерекомендованных криптоактивов попадает большинство криптоактивов, выпущенных в иностранных или в нерегулируемых информационных системах, в частности цифровая валюта.

Применительно к возможности *инвестировать* в обозначенную группу криптоактивов российский законодатель не устанавливает прямых запретов. Банк России с 2017 г. неоднократно обращал внимание граждан и всех участников финансового рынка на повышенные риски при использовании и инвестировании в криптовалюты, указывая на то, что операции с криптовалютами несут в себе высокие риски как при проведении обменных операций, в том числе из-за резких колебаний обменного курса<sup>14</sup>, но прямым образом не ограничивал инвестиционные возможности заинтересованных участников<sup>15</sup>.

В 2021 г. в Информационном письме № ИН-06-59/52 Банк России фактически нивелировал возможность инвестирования в цифровую валюту (криптовалюту) через организаторов торговли и профессиональных участников рынка ценных бумаг, в том числе через институциональных инвесторов (далее — профессиональные участники).

Так, в Информационном письме № ИН-06-59/52 Банк России рекомендует организаторам торговли отказываться в допуске к организованным торгам ценных бумаг российских и иностранных эмитентов, права владельцев на получение выплат по которым зависят от изменения курсов цифровых валют, цен на иностранные цифровые права, цен на цифровые права, которые предлагаются и (или) могут быть приняты в качестве средства платежа, а профессиональным участникам рекомендует отказываться от предложения клиентам — физическим лицам, не являющимся квалифицированными инвесторами, приобретать указанные ценные бумаги, управляющим компаниям воздерживаться от их включения в состав ПИФ (АИФ), инвестиционные паи которых не ограничены в обороте.

<sup>14</sup> Информация Банка России от 4 сентября 2017 г. «Об использовании частных «виртуальных валют» (криптовалют)».

<sup>15</sup> Северин В.А., Коржова И.В. Вопросы безопасности при обращении криптовалюты // Вестник Московского университета. Серия 26. Государственный аудит. 2019. № 4. С. 85.

На первый взгляд может показаться, что ограничения, обозначенные в Информационном письме № ИН-06-59/52, не затрагивают квалифицированных инвесторов, однако на практике у профессиональных участников, через которых инвестор приобретает криптоактивы, возникает вопрос: в отношении какого вида ценных бумаг и иных финансовых инструментов, услуг, предназначенных для квалифицированных инвесторов, лицо должно быть признано квалифицированным для того, чтобы профессиональный участник мог, не нарушая рекомендаций Банка России, включить обозначенные финансовые инструменты в состав инвестиционного портфеля заинтересованного лица?

В соответствии с п. 1.1 Указания Банка России от 29 апреля 2015 г. № 3629-У «О признании лиц квалифицированными инвесторами и порядке ведения реестра лиц, признанных квалифицированными инвесторами» (далее — Указание № 3629-У) профессиональный участник рынка ценных бумаг может квалифицировать лицо только в отношении тех ценных бумаг и иных финансовых инструментов, которые предназначены для квалифицированных инвесторов.

Согласно п. 5 ст. 3 Закона о рынке ценных бумаг ценная бумага или производный финансовый инструмент считаются предназначенными для квалифицированных инвесторов, если в соответствии с нормативными актами Банка России сделки с такими ценными бумагами (договоры, являющиеся такими производными финансовыми инструментами) могут совершаться (заключаться) исключительно квалифицированными инвесторами или за счет квалифицированных инвесторов.

В настоящий момент нормативный акт Банка России, относящий ценные бумаги российских и иностранных эмитентов, права владельцев на получение выплат по которым зависят от изменения курсов цифровых валют, цен на иностранные цифровые права, цен на цифровые права, которые предлагаются и (или) могут быть приняты в качестве средства платежа, к инструментам, предназначенным *исключительно* для квалифицированных инвесторов, отсутствует, следовательно, невозможно признать лицо квалифицированным в отношении обозначенных финансовых инструментов.

В качестве закономерного следствия возникает вопрос о том, насколько интересам инвесторов будет отвечать буквальное толкование положения, в соответствии с которым профессиональный участник может предлагать данные финансовые инструменты / приобретать / включать в состав ПИФ (АИФ), инвестиционные паи которых не ограничены в обороте инвесторам, признанным квалифицированным *в отношении любого вида ценных бумаг и иных финансовых инструментов, услуг*, для которых



предусмотрена соответствующая квалификация? Это ли имел в виду Банк России?

На практике мнимая определенность может вызывать сомнения у организаторов торговли и профессиональных участников, следствием чего станет их отказ от работы с цифровыми валютами и связанными с ними финансовыми инструментами / услугами.

Таким образом, действующее регулирование доступа российских инвесторов к инвестированию в криптоактивы содержит ряд существенных недостатков, связанных как с наличием косвенных ограничений на приобретение некоторых классов финансовых инструментов, производных от криптоактивов, включая цифровую валюту (криптовалюту), так и с неэффективной системой предоставления доступа неквалифицированным инвесторам для приобретения криптоактивов, выпущенных в российских информационных системах, не отвечающую потребностям митигации инвестиционных рисков для неквалифицированных инвесторов.

В рамках совершенствования действующей системы предлагается изменить систему лимитов, установленных для инвестирования в криптоактивы (цифровые права), заменив ее системой «тестирования» для неквалифицированных инвесторов по аналогии с системой, которая вводится Законом № 306-ФЗ с 1 октября 2021 г. в отношении ряда сложных финансовых инструментов, на уровне закона и актов Банка России — определить конкретные сделки, финансовые инструменты и услуги, в отношении которых лицо должно быть признано квалифицированным инвестором, для того чтобы иметь возможность инвестировать в любые классы криптоактивов без ограничений, в том числе через организаторов торговли и профессиональных участников.

### **Литература**

1. Жужжалов М.Б. Криптовалюта как имущество — анализ текущего правового статуса / М.Б. Жужжалов, А.Ю. Толкачев // Вестник экономического правосудия Российской Федерации. 2018. № 9.
2. Санникова Л.В. Цифровые активы: правовой анализ : монография / Л.В. Санникова, Ю.С. Харитонова // 4 Принт. 2020. С. 106—107.
3. Северин В.А. Вопросы безопасности при обращении криптовалюты / В.А. Северин, И.В. Коржова // Вестник Московского университета. Серия 26. Государственный аудит. 2019. № 4. С. 85.

**Калганова Мария Викторовна,**

выпускница магистерской программы «Информационные правоотношения  
в инновационной экономике» МГУ имени М.В. Ломоносова  
*mvkalganova7@gmail.com*

## **ИСТОРИЯ РАЗВИТИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ КОММЕРЦИАЛИЗАЦИИ РЫНКА ИНФОРМАЦИИ В РОССИИ**

Работа посвящена истокам возникновения и дальнейшего развития терминологии и ключевых проблем правового регулирования коммерциализации информации в России, поисков путей их решения, а также актуальности их разрешения сегодня.

**Ключевые слова:** информация, коммерциализация, гражданский оборот, информационное право.

**Mariya V. Kalganova,**

Master, Specialization: Information Legal Relations in the Innovation Economy,  
Lomonosov MSU

## **HISTORY OF DEVELOPMENT OF LEGAL REGULATION OF COMMERCIALIZATION OF INFORMATION MARKET IN RUSSIA**

The article is devoted to the origins and further development of terminology and key problems of legal regulation of commercialization of information in Russia, also to the search for ways to solve them, as well as to the relevance of their solution nowadays.

**Keywords:** information, commercialization, civil turnover, information law.

В современном информационном обществе одну из основных ценностей представляют знания и информация. Деятельность ключевых общественных и государственных институтов направлена на их производство, распространение, распределение, поиски путей коммерциализации и обеспечения, в том числе правового. Развитые и развивающиеся страны перестраивают экономику на инновационный путь развития, в котором нематериальная сфера хозяйственной деятельности занимает центральное место, а в основе создания общественного богатства лежат образование, исследования и инновации.

«Информация — кислород современного мира», — знаменитый афоризм Роналда Рейгана, в котором описана суть значения информации в современном обществе.

Сегодня информация становится товаром и объектом коммерциализации — деятельности по вовлечению в экономический оборот, подчиненной целям извлечения прибыли<sup>1</sup>, а следовательно, и объектом гражданских правоотношений. В этой связи изучение вопросов правового регулирования коммерциализации информации в инновационной экономике России представляется весьма актуальным.

Информация как предмет общественных отношений известна так же давно, как и сами человеческие отношения. Но значение самостоятельного предмета в системе правовых отношений информация приобрела только в середине XX века.

Объективные и субъективные процессы, протекающие в настоящее время в обществе, способствовали тому, что информация приобрела значение товара, стала наивысшим ресурсом, который продается и покупается. Сама жизнь указала на необходимость создания отдельного правового регулирования отношений по поводу информации.

В истории развития цивилизации информация всегда играла определяющую роль и служила основой для принятия решений на всех уровнях и этапах развития общества и государства.

В истории общественного развития традиционно выделяют пять информационных революций, связанных с кардинальными изменениями в сфере производства, обработки и обращения информации, приведших к радикальным преобразованиям общественных отношений. В результате таких преобразований общество приобретало в определенном смысле новое качество.

Сегодня мы переживаем пятую информационную революцию, связанную с интеграцией средств и процессов по всему миру в единую информационную инфраструктуру, в которой активно действуют юридические и физические лица, органы государственной власти и местного самоуправления<sup>2</sup>.

Ученые говорят о формировании общества нового типа — информационного общества. В соответствии с концепцией Д. Белла, З. Бжезинского, О. Тоффлера, поддерживаемой и другими зарубежными учеными, информационное общество — разновидность постиндустриального общества, в котором доминирует новый информационный сектор экономики, а в основе общественного богатства лежат знания и информация<sup>3</sup>.

На международном уровне принципы создания информационного общества и подходы к его созданию впервые были определены

<sup>1</sup> Райзберг Б.А., Лозовский Л.Ш., Стародубцева Е.Б. Современный экономический словарь. 2-е изд., испр. М. : ИНФРА-М, 1999.

<sup>2</sup> Копылов В.А. Информационное право : учебник. 2-е изд., доп. М. : Юрист, 2002. С. 10–11.

<sup>3</sup> Лаврик Н.В. Теоретические концепции информационного общества как предпосылки к зарождению электронной демократии // Вестник ЗабГУ. 2014. № 11. С. 56–65.

в 2000 г. в Окинавской хартии глобального информационного общества<sup>4</sup>, принятой странами «Большой восьмерки». Затем в 2003 г. в Женеве состоялась Всемирная встреча на высшем уровне по вопросам информационного общества, в результате которой были приняты Декларация принципов «Построение информационного общества — глобальная задача в новом тысячелетии»<sup>5</sup>, План действий<sup>6</sup> и Тунисская программа для информационного общества<sup>7</sup>. В основе данных документов лежит ст. 19 Всеобщей декларации прав человека, в которой закреплено право на информацию — свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ<sup>8</sup>.

В развитие вышеуказанных международных стратегических документов в России в 2008 г. Президентом РФ утверждена Стратегия развития информационного общества в Российской Федерации<sup>9</sup>, определившая направления развития информационного общества в России и положившая начало интенсивному использованию органами государственной власти РФ, бизнесом и гражданами информационных и коммуникационных технологий.

Актуальным на сегодняшний день документом в данной сфере является Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденная Указом Президента РФ от 9 мая 2017 г. № 203.

Фундаментальную основу данных документов в РФ составляет Конституция РФ. В соответствии с п. 4 ст. 29 Конституции РФ каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

В развитие конституционной нормы и в поддержку развивающихся отношений в информационной сфере в 1995 г. был принят Федеральный закон «Об информации, информатизации и защите информации». Он заложил начала формирования новой отрасли законодательства, ознаменовал создание механизма правового регулирования в информационной сфе-

<sup>4</sup> Окинавская хартия глобального информационного общества (принята на о. Окинава 22.07.2000) // Дипломатический вестник. 2000. № 8. С. 51–56. Доступ из СПС «КонсультантПлюс».

<sup>5</sup> Декларация принципов «Построение информационного общества — глобальная задача в новом тысячелетии» от 12.12.2003 // URL: <https://www.un.org/> (дата обращения: 10.10.2020).

<sup>6</sup> План действий от 12.12.2003 // URL: <https://www.un.org/> (дата обращения: 10.10.2020).

<sup>7</sup> Тунисская программа для информационного общества от 15.11.2005 // URL: <https://www.un.org/> (дата обращения: 10.10.2020).

<sup>8</sup> Всеобщая декларация прав человека (принята Генеральной Ассамблей ООН 10.12.1948) // СПС «КонсультантПлюс».

<sup>9</sup> Стратегия развития информационного общества в Российской Федерации (утв. Президентом РФ 07.02.2008 № Пр-212) // СПС «КонсультантПлюс».

ре, засвидетельствовал особое значение информации в системе правоотношений<sup>10</sup>.

Впервые на законодательном уровне было закреплено определение понятия информация — сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

В настоящее время указанный закон отменен в связи с принятием Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — Закон об информации). В новом законе определение информации сформулировано более лаконично: «сведения, сообщения или данные независимо от формы их представления».

К концу XX века также сформировались начала юридической науки информационного права. В России в первую очередь она связана с именами таких ученых, как В.А. Копылов<sup>11</sup>, М.М. Рассолов<sup>12</sup>, И.Л. Бачило<sup>13</sup> и др.

Как отмечает И.Л. Бачило, наука информационного права еще молода и развивается под влиянием многих факторов, ориентирована на восприятие различных направлений философского, политологического, социологического осмысления современных процессов продвижения новых технологий информатики<sup>14</sup>. Вместе с тем представляется, что именно результаты научных исследований в данной области дадут мощный толчок к разрешению концептуальных проблем существующего механизма правового регулирования в данной сфере, будут способствовать гармоничному развитию информационного законодательства, соответствующего общественным и государственным интересам.

Таким образом, сегодня в полной мере можно говорить об информационном праве как о самостоятельной отрасли права, представляющей собой правовой фундамент информационного общества и инновационной экономики.

Ученые отмечают комплексный характер данной отрасли, определяя ее как систему норм и отношений, охраняемых силой государства, возникающих в сфере производства, преобразования и потребления информации. Основной предмет правового регулирования информационного права — информационные отношения, возникающие при осуществлении процессов производства, сбора, обработки, накопления, хранения, поиска, передачи, распространения и потребления информации<sup>15</sup>.

<sup>10</sup> Горбачева Е.В. История информационного законодательства. XX век. Начало. // Правовая информатика. 2016. № 3. С. 30–34.

<sup>11</sup> Копылов В.А. Информационное право : учебник.

<sup>12</sup> Рассолов М.М. Информационное право : учебное пособие. М. : Юристь, 1999.

<sup>13</sup> Бачило И.Л. Информационное право. Основы практической информатики : учебное пособие. М. : Юринформцентр, 2001.

<sup>14</sup> Бачило И.Л. Информационное право. С. 31–32.

<sup>15</sup> Копылов В.А. Информационное право : учебник. С. 45.

Возвращаясь к рассмотрению узлового вопроса развития представлений об информации как о правовой категории, необходимо отметить, что в настоящее время в науке и в официальных документах сложилось большое количество подходов к определению понятия информации.

Выделяют следующие концепции информации, встречающиеся в юридической литературе: техноцентрическая концепция — информация приравнивается к данным; антропоцентрическая концепция — информация представляет собой какие-либо сведения об окружающей действительности независимо от формы их выражения; витальная концепция — информация является совокупностью закодированных сведений, необходимых для принятия решений и их реализации; интеграционная концепция — информация трактуется как смысл (понимание, представление, интерпретация), возникающий у человека в результате получения им данных, взаимоувязанный с предшествующими знаниями, понятиями; недетерминированный подход, предполагающий принципиальный отказ от определения понятия информации в качестве одной из основополагающих и первичных категорий, наряду с энергией и материей<sup>16</sup>.

Процесс правового регулирования информации объективно представляется весьма непростым, поскольку информация сама по себе является одним из сложнейших общественных явлений.

Как уже было отмечено ранее, в российском законодательстве определение понятия «информация» закреплено в ст. 2 Закона об информации, из которого следует, что информация — это сведения (сообщения, данные) независимо от формы их представления.

О.В. Кириченко делает вывод о том, что из законодательного определения следует, что информация не может быть объектом правоотношений безотносительно к ее содержанию. Информации как объект права должна быть идентифицируемой и обособляемой. Обособлен может быть как определенный круг информации (например, техническая информация), так и неопределенный (например, любые сведения, имеющие действительную или потенциальную ценность в силу их неизвестности третьим лицам)<sup>17</sup>.

Юридическая наука выработала несколько положений, являющихся ключевыми в определении места информации в правовых отношениях. Во-первых, правоотношения в информационной сфере характеризуются через указание на то, что такие правоотношения возникают в связи и по поводу действий с информацией. Во-вторых, единственным существенным признаком правоотношений в информационной сфере являет-

<sup>16</sup> Мирских И.Ю., Мингалева Ж.А. К вопросу о правовом регулировании информации в условиях информационной экономики // Вестник Пермского университета. Юридические науки. 2017. № 4. Доступ из СПС «КонсультантПлюс».

<sup>17</sup> Кириченко О.В. Информация как объект гражданских правоотношений // Современное право. 2014. № 9. Доступ из СПС «КонсультантПлюс».

ся их объект — определенного вида материальные, духовные и социальные блага, связанные с информацией как результат поведения участника правоотношения (предоставление, получение, неразглашение информации и т.п.)<sup>18</sup>.

В ст. 5 Закона об информации обозначены ключевые характеристики информации как объекта правовых отношений. В зависимости от категории доступа она подразделяется на общедоступную и информацию ограниченного доступа. Последняя устанавливается федеральными законами с обязательным соблюдением режима конфиденциальности. В частности, отношения, связанные с защитой информации, составляющей государственную тайну, регулируются Законом РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне»; отношения, связанные с защитой информации, составляющей коммерческую тайну, регулируются Федеральным законом от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» и т.д.

Информация может являться объектом публичных, гражданских и иных правовых отношений. Последний постулат становится основанием для рассмотрения вопроса оборота информации, который в настоящее время приобретает особую актуальность в условиях формирования инновационной экономики в России.

Таким образом, история развития представлений об информации как правовой категории имеет длинный путь. Вектор развития общества потребовал создания механизма правового регулирования отношений, возникающих по поводу информации и связанных с ней. Информация в современном мире является объектом правоотношений, сформирована отдельная комплексная отрасль права, находящаяся в постоянном развитии. Представляется, что информационное право сможет стать правовым фундаментом для развития инновационной экономики информационного общества.

В контексте современных реалий мы наблюдаем, как информация в том или ином виде становится товаром в экономическом смысле, объектом гражданского оборота и коммерциализируется.

«Кто владеет информацией — тот владеет миром» — афоризм, который сегодня представляет интерес не только с точки зрения актуальности значения, но и с позиции определения гражданско-правовых институтов, регулирующих информационные отношения, справедливости применения к информации одного из ключевых понятий вещного права — «владение».

Попытки однозначно решить вопрос о том, является ли информация объектом гражданских прав, отмечаются с начала формирования механизма правового регулирования информационных отношений в России.

<sup>18</sup> Кириченко О.В. Информация как объект гражданских правоотношений.

На законодательном уровне в разное время были урегулированы два диаметрально противоположных подхода к данному вопросу. В этой связи историю вопроса можно разделить на два периода: с 1995 г. по 2007 г., с 2008 г. до настоящего времени.

Первый подход был обозначен в первоначальной редакции ч. 1 Гражданского кодекса РФ (далее — ГК РФ), вступившей в силу 1 января 1995 г. На протяжении 13 лет согласно ст. 128 ГК РФ информация признавалась на законодательном уровне самостоятельным объектом гражданских прав, далее упоминалась в ст. 139 ГК РФ в контексте правового регулирования режима служебной или коммерческой тайны.

Второй подход связан со вступившими в силу с 1 января 2008 г. изменениями в ГК РФ, внесенными Федеральным законом от 18 декабря 2006 г. № 231-ФЗ «О введении в действие части четвертой Гражданского кодекса Российской Федерации», в результате которых в действие введена часть 4 ГК РФ о правах на результаты интеллектуальной деятельности и средства индивидуализации, а информация исключена из перечня объектов гражданских прав, закрепленных в ст. 128 ГК РФ.

Регулирование рассматриваемого вопроса на законодательном уровне нельзя признать однозначным ни в одном из обозначенных периодов, о чем свидетельствуют различные мнения ученых насчет толкования ст. 128 ГК РФ применительно к категории «информация». Дискуссионным сегодня остается вопрос определения гражданско-правовых институтов, приемлемых для регулирования отношений в данной сфере.

И.Л. Бачило указывает, что до внесения изменений в 2007 г. в ГК РФ информационные объекты могли защищаться как институтами вещного права, так и институтом права интеллектуальной собственности, а площадкой для их встречи была категория «имущество», которая относится к материальным и нематериальным объектам<sup>19</sup>. Причем в пользу возможности применения институтов вещного права к обороту информации свидетельствовали понятия «собственник», «владелец» и «пользователь (потребитель)» информационных ресурсов, содержащиеся в Федеральном законе от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации».

Профессор поддерживает данную позицию и после изменений ГК РФ, рассматривая информацию как объект гражданских прав, несмотря на изъятия ст. 128 ГК РФ и отсутствие вышеуказанных субъектов информационных правоотношений в актуальном Законе об информации<sup>20</sup>.

Таким образом, И.Л. Бачило придерживается комплексного подхода к вопросу регулирования информации в гражданском обороте, высказы-

<sup>19</sup> Бачило И.Л. Информационное право. С. 167.

<sup>20</sup> Там же. С. 170.



вается за возможность применения нескольких институтов гражданского права к информации.

Позицию за особый правовой режим информации в гражданском законодательстве первого периода высказывает Л.Б. Ситдикова, аргументируя свое мнение расположением «информации» между «работами и услугами» и «результатами интеллектуальной деятельности» в ст. 128 ГК РФ в редакции до 2008 г.<sup>21</sup> Такая позиция Л.Б. Ситдиковой совпадает с мнением В.А. Дозорцева, приведенным ниже<sup>22</sup>.

Относительно места информации среди объектов гражданских прав в современный период Л.Б. Ситдикова полагает, что законодатель закрепил конструкцию сочетания средств института права собственности и авторского права<sup>23</sup>. Таким образом, позиция И.Л. Бачило разделяется Л.Б. Ситдиковой.

В.А. Копылов в научном труде 2002 г. высказывается о необходимости согласования применения к информации, информационным объектам институтов авторского права и вещной собственности (на основе принципа информационного объекта или двуединства информации и ее носителя), указывает, что сущность гражданского оборота информации заключается в возможности реализовать исключительное право на информацию (на ее содержание), используя сочетание «информационная собственность».

Автор предпринимает попытку «разложить» информацию по триаде правомочий института права собственности: владение, пользование, распоряжение, под «информационной вещью» подразумевает информацию и ее материальный носитель и указывает, что правомочия собственника должны реализовываться совместно с информационными, определяющими право на использование информации<sup>24</sup>.

Российские цивилисты (например, Е.А. Суханов<sup>25</sup>, А.П. Сергеев<sup>26</sup>), не поддерживали с самого начала концепцию применения к категории «информация» вещных прав, отмечая ее нематериальные или «бестелесные» свойства, противоположные главным признакам вещей согласно теории гражданского права, невозможность применения в европейской континентальной правовой системе режим прав (*res incorporales*) к режиму вещей режим прав, присущие правовой системе общего права<sup>27</sup>.

<sup>21</sup> Ситдикова Л.Б. Информация как правовая и как гражданско-правовая категория: статус информации в гражданском праве // Гражданское право. 2007. № 2. С. 42–43.

<sup>22</sup> Дозорцев В.А. Информация как объект исключительных прав // Дело и право. 1996. № 4. С. 27–35.

<sup>23</sup> Ситдикова Л.Б. Информация как правовая и как гражданско-правовая категория.

<sup>24</sup> Копылов В.А. Информационное право : учебник.

<sup>25</sup> Гражданское право : учебник. Т. 1 / под общ. ред. Е.А. Суханова. 3-е изд., перераб. и доп. М. : Волтерс Клувер, 2006.

<sup>26</sup> Сергеев А.П. Право интеллектуальной собственности в Российской Федерации : учебник. 2-е изд., перераб. и доп. М. : Проспект, 1999. С. 620.

<sup>27</sup> Гражданское право : учебник. Т. 1 / под общ. ред. Е.А. Суханова.

Так, Е.А. Суханов считает, что товарный характер и коммерческая ценность информации не превращают ее в вещь, так же как и сама информация не может быть отождествлена с ее материальным носителем. Для охраноспособной коммерческой информации устанавливается режим объекта обязательственного права, охраноспособная информация относится к интеллектуальной собственности<sup>28</sup>. Таким образом, цивилистом отрицается самостоятельность информации в числе объектов гражданских прав.

Впоследствии Е.А. Суханов положительно оценивает изменения в ст. 128 ГК РФ, отмечая при этом, что в гражданском законодательстве в отношении информации речь идет только о ее форме в виде ноу-хау<sup>29</sup>.

Возвращаясь к подходу о применении института интеллектуальной собственности к правоотношениям, связанным с информацией, В.А. Дозорцев указывает, что традиционные исключительные права (авторские, патентные права) никак не распространяются на информацию, для нее нужна отдельная система. Автор считает, что ближе к праву на информацию находится право на ноу-хау, отмечая, однако, их разные правомочия, объекты и субъекты<sup>30</sup>.

В современный период молодые ученые продолжают исследования с целью определения места информации в системе объектов гражданских прав и применимых правовых институтов к регулированию гражданского оборота информации.

В недавних научных работах укрепляется суждение о том, что информация является самостоятельным объектом гражданских прав несмотря на отсутствие прямого указания ст. 128 ГК РФ, при условии соответствия ст. 2 ГК РФ. Вместе с тем ученые приходят к данному умозаключению разными путями. Различаются также их представления о правовых институтах, применимых в гражданском обороте к информации.

В частности, М.А. Рожкова считает, что информация, имеющая экономическую ценность, являясь нематериальным объектом, не может становиться предметом гражданско-правовых сделок и переходить от одного лица к другому. Однако имущественные права на такую информацию оборотоспособны, могут отчуждаться или иным образом переходить от одного лица к другому. С учетом содержания п. 1 ст. 2 ГК РФ регулирование имущественных отношений по поводу информации не может относиться к сфере информационного права. Возникновение субъективных гражданских прав на информацию и оборот прав на информацию должны регламентироваться именно гражданским правом. В конце концов, автор

<sup>28</sup> Там же.

<sup>29</sup> Перспективы развития гражданского законодательства в России: планы и современные реалии : интервью с Е.А. Сухановым от 20 октября 2008 г. // СПС «КонсультантПлюс».

<sup>30</sup> Дозорцев В.А. Информация как объект исключительных прав // Дело и право. 1996. № 4. С. 27–35.

делает вывод о том, что, поскольку перечень объектов гражданских прав в ст. 128 ГК является открытым, действие данной статьи распространяется на любой объект, имеющий экономическую ценность, даже без прямого указания в статье<sup>31</sup>.

А.А. Инюшкин полагает, что для появления гражданских правовых отношений, связанных с информацией и описанных в ст. 5 Закона об информации, необходимо, чтобы информация получила законодательную связь между интеллектуальной собственностью и информацией либо цели ее использования были направлены на отношения, перечисленные в ст. 2 ГК РФ, не выходящие за сферу действия ст. 1 Закона об информации<sup>32</sup>.

Ученые И.Ю. Мирских, Ж.А. Мингалева считают, что понятие «информация» шире понятия «интеллектуальная собственность», так как включает в себя и не охраняемую информацию. Вместе с тем, ввиду того что содержание права на информацию и содержание исключительного права на информационный продукт не совпадают, полагают, что право на информацию заканчивается там, где начинается защита правообладателей на результат интеллектуальной деятельности<sup>33</sup>.

Правовая защита информации должна быть четко увязана с границами регулирования каждого вида информации и статусом информации. Выделение информации как самостоятельного объекта права должно быть обусловлено только ее фактической ценностью и оборотом, а также необходимостью защиты информации как нематериального, свободно распространяемого блага.

Таким образом, как справедливо отмечает профессор И.Ю. Бачило, острота решения рассматриваемых проблем усиливается в связи с задачей развития в России инновационной экономики, успех реализации которой в значительной мере связан с уяснением и освоением потенциала объектов и прав интеллектуальной собственности в информационной сфере<sup>34</sup>.

Итак, проведенное исследование истории развития правового регулирования коммерциализации информации в России позволяет сделать следующие выводы.

1. Информация всегда играла определяющую роль в развитии и жизни общества, однако началом применения понятия «информация»

<sup>31</sup> Рожкова М.А. Информация как объект гражданских прав, или Что надо менять в гражданском праве // Закон.ру. 2018. 6 ноября. URL: [https://zakon.ru/blog/2018/11/06/informaciya\\_kak\\_obekt\\_grazhdanskih\\_prav\\_ili\\_chto\\_nado\\_menyat\\_v\\_grazhdanskom\\_prave](https://zakon.ru/blog/2018/11/06/informaciya_kak_obekt_grazhdanskih_prav_ili_chto_nado_menyat_v_grazhdanskom_prave) (дата обращения: 01.10.2020).

<sup>32</sup> Инюшкин А.А. Информация в системе объектов прав и ее взаимосвязь с интеллектуальной собственностью на примере баз данных // Информационное право. 2016. № 4. Доступ из СПС «КонсультантПлюс».

<sup>33</sup> Мирских И.Ю., Мингалева Ж.А. К вопросу о правовом регулировании информации в условиях информационной экономики.

<sup>34</sup> Бачило И.Л. Информационное право. С. 173.

в качестве правовой категории в России необходимо считать дату вступления в силу основного закона РФ — Конституции РФ, в котором закреплено право человека и гражданина на информацию. Затем был принят специальный Закон об информации, что способствовало формированию новой отрасли законодательства, науки и права в целом.

2. Законодательное определение понятия «информация» содержится в Законе об информации (ст. 2). Оно представляется лаконичным, но широким по смыслу, концентрируется вокруг понятия «сведения» независимо от формы их предоставления.

В этой связи единое понимание «информации» в теории права отсутствует, выделяется несколько концептуальных подходов к определению понятия «информация», включая тезис об отсутствии необходимости ее определения как основополагающей первичной категории.

3. Процесс коммерциализации информации предполагает ее введение в гражданский оборот. Закон об информации подтверждает возможность «информации» быть объектом гражданских правоотношений (ст. 5).

Однако гражданско-правовые нормы, регулирующие правоотношения по данному вопросу, менялись. История вопроса делится на два периода, соответствующих внесению изменений в ст. 129 ГК РФ. В настоящее время информация не значится в перечне самостоятельных объектов гражданских прав, однако признается таковым многими учеными-специалистами в области информационного права.

В науке информационного права также всегда уделялось большое внимание исследованию проблемы определения применимых гражданско-правовых институтов в отношениях, связанных с гражданско-правовым оборотом информации. Обсуждались следующие применимые институты: права собственности и других вещных права, обязательственного права, личных неимущественных прав и интеллектуальной собственности. Кроме того, многие ученые приходят к умозаключению о необходимости обособленного правового регулирования гражданского оборота информации без привязки к конкретному гражданско-правовому институту.

Таким образом, указанный вопрос до настоящего времени является дискуссионным, требующим окончательного решения в теории права и правоприменительной деятельности.

### **Литература**

1. Бачило И.Л. Информационное право. Основы практической информатики : учебное пособие / И.Л. Бачило. Москва : Юринформцентр, 2001.
2. Горбачева Е.В. История информационного законодательства. XX в. Начало / Е.В. Горбачева // Правовая информатика. 2016. № 3. С. 30–34.

3. Гражданское право : учебник. Т. 1 / под общ. ред. Е.А. Суханова. 3-е изд., перераб и доп. Москва : Волтерс Клувер, 2006.
4. Дозорцев В.А. Информация как объект исключительных прав / В.А. Дозорцев // Дело и право. 1996. № 4. С. 27–35.
5. Инюшкин А.А. Информация в системе объектов прав и ее взаимосвязь с интеллектуальной собственностью на примере баз данных / А.А. Инюшкин // Информационное право. 2016. № 4. Доступ из СПС «КонсультантПлюс».
6. Кириченко О.В. Информация как объект гражданских правоотношений / О.В. Кириченко // Современное право. 2014. № 9. Доступ из СПС «КонсультантПлюс».
7. Копылов В.А. Информационное право : учебник. 2-е изд., доп. / В.А. Копылов. Москва : Юрист, 2002.
8. Лаврик Н.В. Теоретические концепции информационного общества как предпосылки к зарождению электронной демократии / Н.В. Лаврик // Вестник ЗабГУ. 2014. № 11. С. 56–65.
9. Мирских И.Ю. К вопросу о правовом регулировании информации в условиях информационной экономики / И.Ю. Мирских, Ж.А. Мингалева // Вестник Пермского университета. Юридические науки. 2017. № 4. Доступ из СПС «КонсультантПлюс».
10. Перспективы развития гражданского законодательства в России: планы и современные реалии : интервью с Е.А. Сухановым от 20 октября 2008 г. // СПС «КонсультантПлюс».
11. Рассолов М.М. Информационное право : учебное пособие / М.М. Рассолов. Москва : Юрист, 1999.
12. Рожкова М.А. Информация как объект гражданских прав, или Что надо менять в гражданском праве / М.А. Рожкова // Закон.ру. 2018. 6 ноября. URL: [https://zakon.ru/blog/2018/11/06/informaciya\\_kak\\_obekt\\_grazhdanskih\\_prav\\_ili\\_chno\\_nado\\_menyat\\_v\\_grazhdanskom\\_prave](https://zakon.ru/blog/2018/11/06/informaciya_kak_obekt_grazhdanskih_prav_ili_chno_nado_menyat_v_grazhdanskom_prave) (дата обращения: 01.10.2020).
13. Сергеев А.П. Право интеллектуальной собственности в Российской Федерации : учебник. 2-е изд., прераб. и доп. / А.П. Сергеев. Москва : Проспект, 1999. 750 с.
14. Ситдикова Л.Б. Информация как правовая и как гражданско-правовая категория: статус информации в гражданском праве / Л.Б. Ситдикова // Гражданское право. 2007. № 2. С. 42–43.

**Ильюшина Инна Сергеевна,**

соискатель кафедры компьютерного права и информационной безопасности  
факультета ВШГА МГУ имени М.В. Ломоносова  
по специальности «Информационное право»  
*ak@defendit.ru*

## ИСТРЕБОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ПРИЕМЕ НА РАБОТУ

Данная статья посвящена рассмотрению вопроса о возможности истребования у соискателя на занятие вакантной должности дополнительных персональных данных сверх тех, которые установлены законодательством. Основываясь на праве работодателя иметь возможность выбора, следует его законный интерес в приеме на работу наиболее подходящего кандидата, для чего он должен располагать более широким кругом информации о человеке, чем та, которую можно получить, ознакомившись с документами, перечисленными в Трудовом кодексе РФ, а также с учетом специфики работы в отдельных федеральных законах, указах Президента РФ и постановлениях Правительства РФ. Автором определена проблематика данного вопроса, связанная с отсутствием его регулирования на законодательном уровне, а также предложены возможные пути его решения.

**Ключевые слова:** информация, персональные данные, работодатель, Трудовой кодекс РФ, кандидат, прием на работу.

**Inna S. Ilyushina**

Applicant for the Department of Computer Law and information security  
Faculty of Higher School of Economics of the Lomonosov Moscow State University  
in the specialty "Information law"

## THE REQUIREMENT OF PERSONAL DATA WHEN RECEIVING TO WORK

This article is devoted to the consideration of the possibility of requesting additional personal data from an applicant for a vacant position in addition to those established by law. Based on the employer's right to have a choice, his legitimate interest in hiring the most suitable candidate follows, for which he must have a wider range of information about a person than that which can be obtained by reading the documents listed in the Labor Code of the Russian Federation, and also taking into account the specifics of work in individual federal laws, decrees of the President of the Russian Federation and decrees of the Government of the Russian Federation. The author defines the problematics of this issue related to the lack of its regulation at the legislative level, and also suggests possible ways of solving it.

**Keywords:** information, personal data, employer, Labor Code of the Russian Federation, candidate, hiring.

Данные, идентифицирующие субъекта, известны с незапамятных времен. Это и дворовое прозвище, впоследствии трансформировавшееся в фамилию, и имя субъекта, и иные, характеризующие его особенности, например, физические. При этом можно смело утверждать, что никогда ранее ни персональным данным, ни вопросам, связанным с их защитой, не предавалось такого значения, как сейчас. Все это является закономерным следствием технологического развития общества, при котором появилась возможность получать много больше информации о субъекте, чем в совсем еще недалеком прошлом. Современные технологии в буквальном смысле способны фиксировать каждый шаг человека, собирать информацию о его предпочтениях, круге общения и т.п. В настоящих реалиях за каждым субъектом тянется свой цифровой след, на основании которого вполне возможно составить его личностный портрет. И это пользуется огромным спросом, например, в целях индивидуализации каких-либо потребительских предложений. Но это, безусловно, не единственная сфера его использования. Практика последних лет упорно свидетельствует о том, что специалисты, осуществляющие работу по подбору персонала, повсеместно мониторят персональную информацию кандидатов, размещенную ими в сети Интернет, например в социальных сетях, на форумах, и эта информация оказывает существенное влияние на выбор работодателя. Так, например, профиль в социальной сети можно смело назвать визитной карточкой человека, поскольку он может содержать фотографию или иной аватар, указывать на статус персоналия. Также имеется возможность усмотреть, какой контент он предпочитает в виде фото, видео, музыки, новостной ленты, что постит и репостит. Все это очень важно и дает работодателю возможность понять, сможет ли претендент вписаться в уже сложившийся коллектив, близки ли ему внутрикорпоративные ценности и т.п. Но при этом он не имеет законной возможности затребовать эти и дополнительные данные от соискателя, поскольку нормы действующего законодательства содержат исчерпывающий перечень документов, предъявляемых при приеме на работу.

Практика требовать от претендента определенные документы и информацию при решении вопроса о его найме возникла достаточно давно и не является новой в данной сфере общественных отношений. Так, статьей 6 Аптекарского Устава от 20 сентября 1789 года предусмотрено, что «для вящей же общества к аптекам доверенности не должен аптекарь принимать в услужение ни провизора, ни гезеля, который государственною медицинскою коллегией или определенным на то штат-физиком во своем знании не одобрен»<sup>1</sup>. Яркий пример необходимости

<sup>1</sup> Аптекарский Устав. Раздел Б. «История фармацевтического сословия». Стр. XXXIII. Извлеченный из Свода законов полных собраний законов, опубликованных циркуляров Министерства внутренних дел, постановлений Медицинского совета и разъясняемый историей законодательства / [соч.] Н. Варядинова, д-р прав и философии,

предоставления документа, свидетельствующего о наличии у претендента специального образования, что сохранило свою актуальность и по сей день. Согласно Циркуляру медицинского департамента 14/18 марта 1857 года № 2.530—2.582<sup>2</sup> постановлено «от фармацевтов всех степеней, при поступлении их на службу при вольных аптеках, а равно при открытии или снятии на аренду аптек, требовать непременно представления свидетельств и удостоверений о поведении и занятии их за все время от получения диплома до последнего места служения. Если кто из фармацевтов объявит, что он некоторое время провел без места, то за это время о добронравном поведении, несостоянии под следствием и судом он должен представить свидетельство от полиции». Циркулярным предложением министра народного просвещения попечителям учебных округов от 3 ноября 1879 года № 12074<sup>3</sup> предусмотрено, что «в целях предупреждения попыток выдерживать испытание на звание аптекарского ученика посредством подставного лица, возбуждено было ходатайство о разрешении применять к лицам, желающим подвергнуться сему испытанию, следующие предосторожности: требовать от экзаменуемого, кроме документов, представления и фотографической своей карточки». Данная карточка впоследствии прикреплялась надлежащим образом к аттестационному документу и заверялась печатью. Здесь мы видим первые попытки применения в общественных правоотношениях биометрических данных человека. Не были обойдены в дореволюционном законодательстве и правила приема на работу в иных сферах деятельности, причем данные требования, что интересно, содержались в Уложении о наказаниях уголовных и исправительных, нарушение которых каралось в порядке уголовного судопроизводства. Так, Уложением о наказаниях уголовных и исправительных 1845 года предусмотрен запрет хозяину фабрики или иного заведения принимать мастерового или работника без надлежащего паспорта или билета<sup>4</sup>. Мастер, который примет к себе ученика другого мастера без письменного свидетельства или отпуска от последнего, подвергался наказанию<sup>5</sup>. Аналогично подлежал наказанию и подмастерье, который отойдет от мастера своего и вступит в службу к другому мастеру, не получив сви-

---

чл. С.-Петербург. и Венского фармацевтического и других ученых обществ. С.-Петербург : Тип. М-ва вн. дел, 1880. 12, LXX. Место хранения оригинала : РГБ. URL: <https://www.rglib.ru/item> (дата обращения: 20.08.2021).

<sup>2</sup> Там же. Устав врачебный. Т. 3. Свод Законов (по продол. 1876 года). Аптекарский Устав. Раздел Ж. Службные списки фармацевтической деятельности. С. 118.

<sup>3</sup> Там же. Раздел А. «Права и обязанности фармацевтов». С. 13. Свод законов. Т. III. Устав врачебный. Раздел А. «Ученые степени и звания».

<sup>4</sup> Уложения о наказаниях уголовных и исправительных 1845 года. Статья 1787. Санкт-Петербург : Типография 2 отделения собственной е.и.в. канцелярии. 574 с. С. 699. Место хранения: РГБ. URL: <https://rusneb.ru/catalog> (дата обращения: 20.08.2021).

<sup>5</sup> Там же. Статья 1797. С. 702.



детельства или отпуска от прежнего<sup>6</sup>. Уложение о наказаниях уголовных и исправительных 1885 года еще больше расширил и круг работодателей, и перечень требований при найме. Так, в статье 388<sup>7</sup> в отдельную категорию выделены чиновные служащие. «Кто заведомо примет или представит к принятию на службу человека, не имеющего права вступить в оную вследствие судебного приговора, или по состоянию и по происхождению своему, или по недостижению положенного на то законом возраста — без соблюдения особых, для определения или принятия таких людей на службу постановленных правил» подлежал наказанию. Здесь появляются дополнительные сведения персонального характера — состояние, происхождение, возраст, без которых лицо не вправе претендовать на занятие каких-либо должностей по государственной службе. Купец, который примет приказчика, не давшего преждему своему хозяину в торговых делах отчета и не имеющего в том свидетельства, также подвергнется уголовному преследованию<sup>8</sup>. Интересная информация появляется в статье 1213<sup>9</sup>, согласно которой хозяин корабля подлежит наказанию за «прием для управление оного корабельщика без письменных свидетельств, предписанных уставами торговыми, или без заключения с ним письменного, по предписанной форме договора, с заявлением оного в маклерских книгах». Аналогичная норма содержится в статье 1235<sup>10</sup> и применяется к корабельщику, который примет на работу штурмана без соблюдения вышеуказанных условий. В данных нормах появляется одно из первых упоминаний о письменных трудовых договорах, которые, несомненно, содержали большое количество информации персонального характера. Статьей 373 Уголовного Уложения 1903 года<sup>11</sup> предусмотрено, что «виновный в найме на сельские работы рабочего, заведомо обязанного на то же время срочным договором найма по договорному листу с другим нанимателем», подлежал наказанию. То есть, исходя из данной нормы права, при найме на работу необходимо было испросить у претендента вышеуказанную информацию, которая также является персональной. На данных примерах, которые не являются исчерпывающими, отчетливо видно, что поступательное развитие общества влекло за собой совершенствование регулятивной функции законодательства, связанной с отношениями по найму и получением необходимой персональной информации о работнике.

<sup>6</sup> Там же. Статья 1823. С. 709.

<sup>7</sup> Уложения о наказаниях уголовных и исправительных 1885 года : издано проф. Имп. Училища правоведения... Н.С. Таганцевым. 5-е изд., доп. Санкт-Петербург : тип. М. Стасюлевича, 1886. [4], 714 с. С. 255. Место хранения: РГБ. URL: <https://www.prlib.ru/item> (дата обращения: 20.08.2021).

<sup>8</sup> Там же. Статья 1183. С. 499.

<sup>9</sup> Там же. С. 457.

<sup>10</sup> Там же. С. 460.

<sup>11</sup> Санкт-Петербург : Государственная типография, изд. Н.С. Таганцев. 1904. 253 с. С. 77. Место хранения: РГБ. URL: <https://rusneb.ru/catalog> (дата обращения: 20.08.2021).

Революционные события положили начало новой эре законотворчества в данной области. Первый Кодекс законов о труде<sup>12</sup> был принят в 1918 году. Осуществление права на труд обеспечивалось отделами распределения рабочей силы, профессиональными союзами и всеми учреждениями РСФСР (ст. 15), что исключало возможность самостоятельного поиска работы. При этом единственным документом, который требовался при оформлении на работу, была трудовая книжка, в которую заносились отметки о произведенных сотрудником работах и полученных вознаграждениях и пособиях (ст. 80). Согласно пункту 5 приложения к статье 80 «Правила о трудовых книжках» в трудовой книжке указывалось: имя, фамилия и время рождения; название и адрес профессионального союза, к которому принадлежит трудящийся; группа и категория, в которую трудящийся зачислен расценочной комиссией. В соответствии с пунктом 8 приложения к статье 80 «Правила о трудовых книжках» последняя с указанными персональными данными подлежала предъявлению по требованию уполномоченным органов того предприятия, учреждения или хозяйства, где работал трудящийся; отдела распределения рабочей силы; профессионального союза; органов рабочего контроля и охраны труда; страховых касс или заменяющих их органов. 30 октября 1922 года с учетом развития общественных отношений в области трудового права был принят второй Кодекс законов о труде<sup>13</sup>. Наем рабочей силы всеми без исключения предприятиями, учреждениями и хозяйствами (государственными, общественными и частными), а равно отдельными нанимателями, производился через подлежащие органы Народного Комиссариата Труда (ст. 7). Здесь по сравнению с КЗоТ 1918 года ничего не изменилось. Однако появилась норма, закрепленная в статье 9, согласно которой трудящиеся могли приглашаться на работу помимо органов Народного Комиссариата Труда в случаях, требующих политического доверия или специальных знаний, связанных с личностью приглашаемого. Данная норма права давала работодателю законное право получать от трудящегося информацию, связанную с его личностью. Целью же обработки вышеуказанных персональных данных, говоря современным языком, было установление наличия политического доверия или специальных знаний. О трудовых книжках, содержащих иные персональные данные, КЗоТ 1922 года ничего не говорил. Единственное упоминание о документе, который мог быть потребован при приеме на работу, содержится

<sup>12</sup> Собрание Указаний и Распоряжений Рабочего и Крестьянского Правительства РСФСР. 1918. № 87-88. Ст. 905. Приложение из учебного пособия И.Я. Киселева «Трудовое право России» (Москва, 2001). URL: <http://hist.msu.ru/labour>Law>kodex> (дата обращения: 21.08.2021).

<sup>13</sup> Кодекс законов о труде РСФСР : принят 30 октября 1922 г. // Собрание Указаний и Распоряжений Рабочего и Крестьянского Правительства РСФСР. 1922. № 70. Ст. 903. Приложение из учебного пособия И.Я. Киселева «Трудовое право России» (Москва, 2001). URL: <http://hist.msu.ru/labour>Law>kodex> (дата обращения: 21.08.2021).

в статье 41, согласно которой если наниматель или заведующий предприятием (администрация) взял у нанявшегося удостоверение личности, то обязан возвратить его по первому требованию нанявшегося. Интересен факт появления в данном КЗоТ норм, пусть и несколько косвенно, но все же связанных с защитой персональных данных. Так, статья 42 предусматривала, что наниматель обязан выдать нанявшемуся по его просьбе удостоверение о том, сколько времени и в какой должности нанявшийся у него работал. Помещение в удостоверение каких-либо условных знаков воспрещалось. Сообщение нанимателями друг другу тайных сведений, направленных на установление условий, на которых могут быть приняты рабочие, также воспрещалось. Следующий КЗоТ 1971 года подобных норм уже не содержал. Что же касается документов, которые работник должен был предъявить при приеме на работу, то их перечень был предусмотрен в Типовых правилах внутреннего трудового распорядка для рабочих и служащих предприятий, учреждений, организаций, утвержденных постановлением государственного комитета совета министров СССР по вопросам труда и заработной платы по согласованию с ВЦСПС 29 сентября 1972 года<sup>14</sup> и в Типовых правилах внутреннего трудового распорядка, утвержденных постановлением Госкомтруда СССР 20 июля 1984 года<sup>15</sup>. Согласно вышеуказанным правилам при приеме на работу администрация предприятия, учреждения, организации была обязана потребовать от поступающего трудовую книжку или справку о последнем занятии, военный билет, паспорт, диплом или иной документ о полученном образовании или профессиональной подготовке, свидетельство о рождении для лиц от 14 до 16 лет, страховое свидетельство государственного пенсионного страхования. Что же касается дополнительной информации персонального характера, то ее источником были всевозможные анкеты и автобиографии, которые массово заполнялись соискателями при поступлении на работу. При этом статья 19 КЗоТ 1971 года содержала указание на запрет требовать при приеме на работу документы, помимо предусмотренных законодательством. Тем не менее заполнение анкет и написание автобиографии являлось обязательным. Все анкеты тех лет содержали вопросы, связанные с личной жизнью трудящегося: о социальном происхождении, составе и членах семьи, о пребывании за границей, о наличии там родственников с ответами на вопросы о том, с какого времени они там пребывают и чем занимаются, о пребывании на оккупированной территории, о привлечении к уголовной ответственности, с указанием времени, когда это произошло, и существа противозаконного деяния и т.п. В анкете образца 1963 года вообще имелась графа, в которой нужно было указать рост, цвет глаз и цвет волос. При этом к анкете в обязательном порядке прилагалась фотография, которая должна была отвечать строго установ-

<sup>14</sup> Бюллетень Госкомтруда СССР. 1972. № 12.

<sup>15</sup> Бюллетень Госкомтруда СССР. 1984. № 11.

ленной форме. Таким образом, отсутствие в законодательстве права работодателя требовать при приеме на работу анкету и автобиографию, то есть дополнительную информацию персонального характера, полностью компенсировалось сложившейся и устоявшейся с 30-х годов практикой и безальтернативностью поведения для работника. В современных же реалиях ситуация в корне изменилась, что нашло свое отражение в главе 14 Трудового кодекса РФ<sup>16</sup> от 30 декабря 2001 года № 197-ФЗ. Соискатель на занятие вакантной должности обязан предоставлять свои персональные данные, содержащиеся в документах, исключительно по перечню, установленному в ст. 65 Трудового кодекса РФ (далее — ТК РФ). Так, согласно данной норме права при заключении трудового договора работодатель вправе потребовать от лица, поступающего на работу, следующие документы: паспорт или иной документ, удостоверяющий личность; трудовую книжку и (или) сведения о трудовой деятельности; документ, подтверждающий регистрацию в системе индивидуального (персонифицированного) учета; документы воинского учета; документ об образовании и (или) о квалификации или наличии специальных знаний; справку о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям (для определенных видов деятельности); справку о том, является или не является лицо подвергнутым административному наказанию за потребление наркотических средств или психотропных веществ без назначения врача либо новых потенциально опасных психоактивных веществ (для определенных видов деятельности). Данный перечень является исчерпывающим и расширительному толкованию не подлежит. Но в то же время данной нормой права предусмотрено, что в отдельных случаях с учетом специфики работы Трудовым кодексом, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации может предусматриваться необходимость предъявления при заключении трудового договора дополнительных документов. В качестве дополнительных документов, но исключительно на основании норм действующего законодательства работодатель вправе требовать: письменное заявление с просьбой о поступлении на гражданскую службу и замещении должности государственной гражданской службы Российской Федерации; собственноручно заполненную и подписанную гражданином Российской Федерации анкету установленной формы с приложением фотографии<sup>17</sup>; личную ме-

<sup>16</sup> Трудовой Кодекс Российской Федерации от 31 декабря 2001 г. № 197 (ред. от 28.06.2021) // СЗ РФ. 2002. № 1 (часть 1). Ст. 3. URL: <http://www.consultant.ru> (дата обращения: 21.08.2021).

<sup>17</sup> Указ Президента РФ от 30 мая 2005 г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела» // Российская газета. 2005. 7 июня. URL: <http://www.consultant.ru> (дата обращения: 21.08.2021).

дицинскую книжку<sup>18</sup>; справку о пройденном медицинском обследовании<sup>19</sup> или психиатрическом освидетельствовании<sup>20</sup>; документы о прохождении профессионального отбора<sup>21</sup>; сведения о доходах, об имуществе и обязательствах имущественного характера, а также о доходах, об имуществе и обязательствах имущественного характера супруга (супруги) и несовершеннолетних детей<sup>22</sup>; справку о характере и условиях труда по основному месту работы<sup>23</sup>; медицинское заключение<sup>24</sup>; медицинское освидетельствование<sup>25</sup>; анкету, содержащую биографические сведения о кандидате<sup>26</sup>; документ о соответствии квалификационным требованиям или положениям профессиональных стандартов<sup>27</sup>; справку об отсутствии определенных видов заболеваний и решения комиссии по делам несовершеннолетних и защите их прав<sup>28</sup>; результаты аттестации<sup>29</sup>; о религиозных убеждениях работника<sup>30</sup>; СНИЛС<sup>31</sup>; сведения об адресах сайтов и (или)

<sup>18</sup> Федеральный закон от 30 марта 1999 г. № 52-ФЗ «О санитарно-эпидемиологическом благополучии», ст. 34 // Российская газета. 1999. 6 апреля; Приказ Роспотребнадзора от 20 мая 2005 г. № 402-ФЗ «О личной медицинской книжке» // Российская газета. 2005. 30 июня.

<sup>19</sup> Трудовой кодекс РФ от 31 декабря 2001 г. № 197 (ред. от 28.06.2021), ст. 69, 266, 348.3 // СЗ РФ. 2002. № 1 (часть 1). Ст. 3. URL: <http://www.consultant.ru> (дата обращения: 21.08.2021).

<sup>20</sup> Там же. Ст. 213; Постановление Правительства РФ от 23 сентября 2002 г. № 695 «О прохождении обязательного психиатрического освидетельствования работниками, осуществляющими отдельные виды деятельности, в том числе деятельность, связанную с источниками повышенной опасности (с влиянием вредных веществ и неблагоприятных производственных факторов), а также работающими в условиях повышенной опасности» // Российская газета. 2002. 2 октября.

<sup>21</sup> Там же. Ст. 328.

<sup>22</sup> Там же. Ст. 275, 349.1; Федеральный закон от 27 июля 2004 г. № 79-ФЗ (ред. от 08.12.2020) «О государственной гражданской службе РФ». Ст. 20 // СЗ РФ. 2004. № 31. Ст. 3215.

<sup>23</sup> Трудовой кодекс РФ от 31 декабря 2001 г. № 197 (ред. от 28.06.2021) Ст. 283 // СЗ РФ. 2002. № 1 (часть 1). Ст. 3. URL: <http://www.consultant.ru> (дата обращения: 21.08.2021).

<sup>24</sup> Там же. Ст. 324.

<sup>25</sup> Статья 4.1 Закона РФ от 26 июня 1992 г. № 3132-1 (ред. от 08.12.2020, с изм. от 30.12.2020) «О статусе судей в Российской Федерации». Ст. 4.1 // Российская газета. 1992. 29 июля.

<sup>26</sup> Там же. Ст. 5; Федеральный закон от 30 ноября 2011 г. № 342-ФЗ (ред. от 08.12.2020) «О службе в органах внутренних дел Российской Федерации». Ст. 18 // Российская газета. 2011. 7 декабря.

<sup>27</sup> Трудовой кодекса РФ от 31 декабря 2001 г. № 197 (ред. от 28.06.2021). Ст. 330.2 // СЗ РФ. 2002. № 1 (часть 1). Ст. 3. URL: <http://www.consultant.ru> (дата обращения: 21.08.2021).

<sup>28</sup> Там же. Ст. 331.

<sup>29</sup> Там же. Ст. 336.1.

<sup>30</sup> Там же. Ст. 344. Несмотря на то что имеется законодательный запрет на обработку персональных данных о религиозных убеждениях (ст. 10 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», ст. 86 Трудового кодекса РФ), все же при принятии на работу в религиозную организацию данный вопрос приобретает одно из первостепенных значений, поскольку статьей 24 Федерального закона от 26 сентября 1997 г. № 125-ФЗ «О свободе совести и о религиозных объединениях» религиозные организации вправе устанавливать в соответствии со своими внутренними установлениями условия деятельности священнослужителей и религиозного персонала, а также требования к ним, в том числе в части религиозного образования. См.: Российская газета. 1997. 1 октября.

<sup>31</sup> Федеральный закон от 1 апреля 1996 г. № 27-ФЗ (ред. от 20.07.2020) «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования». П. 3 ст. 9 // Российская газета. 1996. 10 апреля.

страниц сайтов в информационно-телекоммуникационной сети «Интернет», на которых гражданин, претендующий на замещение должности гражданской службы, гражданский служащий размещали общедоступную информацию, а также данные, позволяющие их идентифицировать<sup>32</sup>; данные об обязательной государственной дактилоскопической регистрации<sup>33</sup>. Как видно из вышеизложенного, речь идет исключительно о документе — материальном носителе с зафиксированной на нем в любой форме информацией в виде текста, изображения и (или) их сочетании, который имеет реквизиты, позволяющие его идентифицировать, и предназначен для передачи во времени и в пространстве в целях общественного использования и хранения<sup>34</sup>. Требовать же от лица, поступающего на работу, иные документы, помимо предусмотренных Трудовым кодексом, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации, запрещается<sup>35</sup>.

Безусловно, все вышеуказанные документы содержат в себе информацию персонального характера, но формально это документы, а не информация. При этом в действующем трудовом законодательстве, наряду с отсутствием прямого запрета, никак не урегулирована возможность работодателя запрашивать от претендента на занятие вакантной должности, помимо вышеуказанных документов, дополнительную информацию персонального характера, связанную с предполагаемыми трудовыми отношениями. Современная действительность информационного общества давно и настоятельно требует адаптировать законодательство данной отрасли права к имеющимся реалиям. Вышеуказанный минимально достаточный набор задокументированных сведений уже давно перестал соответствовать и потребностям бизнес-сообщества, и требованиям государственных структур, что, на наш взгляд, повлекло за собой дополнение Федерального закона от 27 июля 2004 года № 79-ФЗ «О государственной гражданской службе Российской Федерации» статьей 20.2, согласно которой граждане, претендующие на замещение должности гражданской службы, должны предоставить сведения об адресах сайтов и (или) страниц сайтов в ИТС «Интернет», на которых гражданин размещал общедоступ-

<sup>32</sup> Федеральный закон от 27 июля 2004 г. № 79-ФЗ (ред. от 08.12.2020) «О государственной гражданской службе РФ». Ст. 20, 20.2 // СЗ РФ. 2004. № 31. Ст. 3215.

<sup>33</sup> Статья 9 Федерального закона от 25 июля 1998 г. № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации» содержит перечень лиц, для которых прохождение данной регистрации при приеме на работу является обязательным. См.: Российская газета. 1998. 1 августа.

<sup>34</sup> Федеральный закон от 29 декабря 1994 г. № 77-ФЗ «Об обязательном экземпляре документов» // Российская газета. 1995. 17 января.

<sup>35</sup> Трудовой кодекс РФ от 31 декабря 2001 г. № 197 (ред. от 28.06.2021). Ст. 65 // СЗ РФ. 2002. № 1 (часть 1). Ст. 3. URL: <http://www.consultant.ru> (дата обращения: 21.08.2021).

ную информацию, а также данные, позволяющие их идентифицировать, за три календарных года, предшествовавших году поступлению на гражданскую службу. Введение данной нормы права, на наш взгляд, обусловлено и возможностью дополнительной проверки, поскольку социальные сети и иная информация в сети Интернет зачастую способна дать более правдивый профайл кандидата, и заботой о репутационных рисках государственной структуры в связи с приемом на работу того или иного кандидата. Так, например, какие-то неосторожные фото или видео сотрудников государственных структур, выложенные в сети Интернет, вполне способны скомпрометировать эти самые структуры, что нередко наблюдается в последнее время. Действительно, гражданский служащий обязан не совершать поступки, порочащие его честь и достоинство<sup>36</sup>, что нашло свое закрепление на законодательном уровне. Но это не говорит о том, что бизнес не заботится о своем имидже, хотя упоминание об этом на уровне нормативно-правового регулирования отсутствует. Исходя из того, что предпринимательская деятельность осуществляет на свой страх и риск<sup>37</sup>, репутационные потери частной структуры могут в некоторых случаях означать конец ее существования. Но при этом «бизнес», в отличие от государственных структур, на законодательном уровне лишен возможности запрашивать у кандидата на занятие вакантной должности сведения о его активности в сети Интернет, что при наличии одинаковых целей при приеме на работу ставит его в неравное положение, а это нельзя признать ни законным, ни обоснованным.

Основной целью при обработке персональных данных в организациях является соблюдение прав и свобод человека и гражданина, что прямо предусмотрено в ст. 86 ТК РФ. В отношениях, связанных с обработкой персональных данных, приоритет отдан основным конституционным правам личности с некоторыми изъятиями в пользу каких-либо государственных или общественных интересов. Основываясь на праве работодателя иметь возможность выбора, следует его законный интерес в приеме на работу наиболее подходящего кандидата, для чего он должен располагать более широким кругом информации о человеке, чем та, которую можно получить, ознакомившись с документами, перечисленными в ст. 65 ТК РФ, а также с учетом специфики работы в отдельных федеральных законах, указах Президента РФ и постановлениях Правительства РФ. Отсутствие такой возможности существенно затрудняет выбор, поскольку при предоставлении несколькими соискателями абсолютно одинакового набора документов невозможно сделать желательный и осознанный

<sup>36</sup> Федеральный закон от 27 июля 2004 г. № 79-ФЗ (ред. от 08.12.2020) «О государственной гражданской службе РФ». Подп. 8 п. 1 ст. 18. Ст. 20 // СЗ РФ. 2004. № 31. Ст. 3215.

<sup>37</sup> Гражданский кодекс РФ (ред. от 08.07.2021). Подп. 1 ст. 2 // СЗ РФ. 1994. № 32. Ст. 3301.

выбор без получения дополнительной информации о кандидате. В современных реалиях наблюдается усиление конкурентности на рынке труда, которая отчасти обусловлена и тем, что в интересах и кандидата, и работодателя представить и получить наиболее значимое количество информации о соискателе. Часть информации претендент предоставляет по собственной инициативе, например, в резюме, другую часть — по просьбе работодателя. Все это происходит довольно хаотично, что может привести и приводит к нарушению прав человека и гражданина в области получения и обработки персональных данных. Разрешение данной проблемы возможно на уровне как федерального законодательства, так и на уровне локального нормотворчества. Так, в ТК РФ следует легально закрепить еще одну цель обработки персональных данных, связанную с выявлением и определением кандидата на занятие вакантной должности с наиболее эффективными показателями. Для работодателя же следует предусмотреть обязанность утверждения политики персональных данных в части определения перечня и объема дополнительной информации, которая с учетом специфики вакантной должности необходима последнему для выявления наиболее подходящей кандидатуры и устранения возможных имиджевых потерь.

Внесение вышеуказанных изменений в трудовое законодательство позволит также разрешить проблему, связанную с порядком получения такой информации. В Трудовом кодексе защите персональных данных посвящена глава 14, где речь идет исключительно о работниках, коими согласно положениям статьи 20 Трудового кодекса являются физические лица, вступившие в трудовые отношения с работодателем. В ситуации же, при которой лицо является не работником, поскольку трудовой договор с ним не заключен и он не приступил к исполнению трудовых обязанностей, а лишь претендентом на занятие вакантной должности, положения главы 14 Трудового кодекса неприменимы, в связи с чем руководствоваться следует иными нормами права. Согласно положениям п. 1 ст. 9 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»<sup>38</sup> субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Данная норма права дает нам два понятия — предоставление персональных данных и их обработка. Под обработкой персональных данных вышеуказанная норма права понимает любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, системати-

<sup>38</sup> Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 02.07.2021) «О персональных данных» // СЗ РФ. 2006. № 31 (часть 1). Ст. 3451.



зацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных. Поскольку персональные данные могут быть обезличены, удалены, уничтожены, то последние должны быть зафиксированы на каком-то носителе. Совершенно очевидно, что проделать данные манипуляции с персональными данными, если они находятся исключительно в сознании у человека, нельзя. В этой связи устные интервью, собеседование с претендентом на занятие вакантной должности, на которых последний принимает решение о предоставлении своих персональных данных, обработкой персональных данных априори считаться не могут. Далее необходимо рассмотреть вопрос о том, какую же информацию о претенденте на занятие вакантной должности работодатель не имеет права обрабатывать ни при каких условиях, за исключением случаев, когда соискатель дает на это свое согласие. При этом именно обрабатывать, а не просто получать устные ответы на такие же вопросы. Прежде всего следует обратиться к положениям ст. 23 и 24 Конституции РФ<sup>39</sup>, являющейся законом прямого действия и имеющей высшую юридическую силу. Так, Конституция гарантирует, что каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Своим определением от 9 июня 2005 г. по делу №248-О<sup>40</sup> Конституционный Суд Российской Федерации разъяснил, что право на неприкосновенность частной жизни (ст. 23, ч. 1, Конституции Российской Федерации) означает предоставленную человеку и гарантированную государством возможность контролировать информацию о самом себе, препятствовать разглашению сведений личного, интимного характера. В понятие «частная жизнь» включается та область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если она носит непротивоправный характер. Часть 1 ст. 10 Закона о персональных данных налагает запрет на обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Последнее возможно только с письменного согласия соискателя на обработку его персональных данных. Таким образом, законодательство, действующее на территории Российской Федерации, не запрещает работо-

<sup>39</sup> Конституция Российской Федерации (ред. от 14.03.2020) // Официальный текст Конституции РФ с внесенными поправками от 14.03.2020 опубликован на Официальном интернет-портале правовой информации <http://www.pravo.gov.ru>, 04.07.2020.

<sup>40</sup> URL: [http://www.consultant.ru>cons\\_doc\\_LAW\\_54736](http://www.consultant.ru>cons_doc_LAW_54736)

дателю получать от соискателя информацию персонального характера, включая специальную категорию персональных данных, но только при наличии согласия последнего. Но в любом случае с целью избежания злоупотреблений со стороны работодателя для последнего следует на законодательном уровне предусмотреть обязанность утверждения политики персональных данных в части определения перечня и объема дополнительной информации, которая с учетом специфики вакантной должности необходима последнему для выявления наиболее подходящей кандидатуры.

### **Литература**

1. Лушникова М.В. Очерки теории трудового права / М.В. Лушникова, А.М. Лушников. Санкт-Петербург : Издательство Р. Асланова «Юридический центр Пресс», 2006. 940 с.
2. Киселев И.Я. Трудовое право России. Историко-правовое исследование : учебное пособие / И.Я. Киселев. М. : Норма, 2001. 384 с.
3. Северин В.А. Методика правового обеспечения безопасности персональных данных в организациях / В.А. Северин // Вестник Московского университета. Серия 11. 2021. № 3. С. 49–61.
4. История социально-трудовых отношений в России. Санкт-Петербург : СПбГУП, 2020. 248 с.

**Робсман Юлия Владимировна,**  
Банк России,  
соискатель кафедры компьютерного права и информационной безопасности  
МГУ имени М.В. Ломоносова

## **ПРОБЛЕМЫ РЕГУЛИРОВАНИЯ ИНСАЙДЕРСКОЙ ИНФОРМАЦИИ В ЗАКОНОДАТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ**

В статье рассматриваются проблемы регулирования инсайдерской информации в законодательстве Российской Федерации, проводится сравнительный анализ защиты инсайдерской информации в мире и в России. Сравнительно молодое «антиинсайдерское» законодательство Российской Федерации нуждается в развитии и синхронизации с мировым. В статье исследуются основные проблемы действующего регулирования и предлагаются возможные варианты их решения.

**Ключевые слова:** инсайдерская информация, инсайдер, раскрытие информации, перечень инсайдерской информации, мягкое регулирование, иностранный эмитент.

**Yulia V. Robsman**  
Bank of Russia,  
Candidate of the Department of Computer Law and Information Security  
of the Lomonosov Moscow State University

## **PROBLEMS OF REGULATION OF INSIDER INFORMATION IN RUSSIA**

The article discusses problems of regulation of insider information in the legislation of Russia, also contains the comparative analysis of protection of insider information in Russia and in other countries. The relatively young “anti-insider” legislation in Russia needs development and synchronization with the international legislation. The article discusses the main problems of regulation of insider information and proposes possible options of their solution.

**Keywords:** insider information, insider, disclosure of information, list of insider information, soft regulation, foreign issuer.

Регулирование инсайдерской информации возникло в первой половине 20 века. Исторически первой страной, признавшей незаконными сделки, совершенные с использованием инсайдерской информации, стали США, где соответствующие нормы появились уже в 1934 г.

Позднее в 20 веке регулирование инсайдерской информации было имплементировано в законодательство большинства развитых стран.

Вместе с тем в российском законодательстве тема защиты инсайдерской информации получила свое прямое закрепление только в 2010 г. с принятием Федерального закона от 27 июля 2010 г. № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»<sup>1</sup>.

Федеральный закон № 224-ФЗ впервые закрепил термин «инсайдерская информация». В его отсутствие с 1995 г. к нему фактически был приравнен термин «служебная информация», режим которой регулировала ст. 139 Гражданского кодекса РФ (далее — ГК РФ), утратившая силу с 1 января 2008 г.

При этом отдельные попытки регулирования инсайдерской информации предпринимались значительно ранее.

Так, в 2002 г. в новой редакции Федерального закона «О рынке ценных бумаг»<sup>2</sup> было закреплено понятие «сделки, совершаемые с использованием служебной информации», что сейчас известно как «инсайдерские сделки». В отсутствие законодательного закрепления термина «инсайдер» тем не менее были подробно описаны лица, располагающие служебной информацией (например, члены органов управления эмитента, аудиторы эмитента).

Принятие же специального законодательства об инсайте и манипулировании было мучительно «выстрадано»: законопроект об инсайте обсуждался с 1990-х годов, разные версии документа многократно вносились в Государственную Думу, но ни разу не прошли даже первого чтения. И только разработанный в 2008 г. Федеральной службой по финансовым рынкам законопроект увидел свет в 2010 г.

В соответствии с Федеральным законом № 224-ФЗ под инсайдерской информацией понимается точная и конкретная информация, которая не была распространена (в том числе сведения, составляющие коммерческую, служебную, банковскую тайну, тайну связи (в части информации о почтовых переводах денежных средств) и иная охраняемая законом тайна) и распространение которой может оказать существенное влияние на

<sup>1</sup> Федеральный закон от 27 июля 2010 г. № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» (ред. от 02.07.2021) // СПС «КонсультантПлюс».

<sup>2</sup> Федеральный закон от 28 декабря 2002 г. № 185-ФЗ «О внесении изменений и дополнений в Федеральный закон «О рынке ценных бумаг» и о внесении дополнения в Федеральный закон «О некоммерческих организациях» // СЗ РФ. 2002. № 52 (часть 2). Ст. 5141.

цены финансовых инструментов, иностранной валюты и (или) товаров (в том числе сведения, касающиеся одного или нескольких эмитентов эмиссионных ценных бумаг, одной или нескольких управляющих компаний инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов либо одного или нескольких финансовых инструментов, иностранной валюты и (или) товаров).

Детерминированность признаков инсайдерской информации, а также их оценочный характер формируют сравнительно «размытое» понятие, не способное, как представляется, в полной мере адекватно отвечать целям и задачам противодействия незаконному использованию инсайдерской информации и манипулирования рынком.

Во-первых, спорным является закрепление как инсайдерской информации сведений, составляющих коммерческую, служебную, банковскую тайну, тайну связи (в части информации о почтовых переводах денежных средств) и иную охраняемую законом тайну.

Как верно отмечает С.П. Гришаев, отличие инсайдерской информации от таких видов конфиденциальной информации, как, например, банковская тайна, состоит в том, что банковская тайна подлежит сохранению. Должны быть проведены все допускаемые законом действия для того, чтобы эта информация осталась тайной, чтобы она не стала достоянием неограниченного круга лиц. Инсайдерская же информация на финансовом и товарном рынках, напротив, это та информация, которая должна сохраняться недоступной для третьих лиц достаточно короткое время. Но затем она подлежит обязательному раскрытию<sup>3</sup>.

Действительно, правовой режим такого рода чувствительной информации, как инсайдерская, предполагает необходимость ее незамедлительного раскрытия. Указанное направлено на защиту прав инвесторов путем нивелирования рисков незаконного использования инсайдерской информации в случае ее длительного сохранения в тайне. Так, например, MAR<sup>4</sup> содержит условие, что обнародование внутренней информации эмитентом необходимо во избежание инсайдерских сделок и гарантии того, что инвесторы не будут введены в заблуждение. В этой связи эмитенты должны обнародовать внутреннюю информацию в кратчайшие сроки.

<sup>3</sup> Гришаев С.П. Комментарий к Федеральному закону от 27 июля 2010 г. № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс», 2010.

<sup>4</sup> Регламент № 596/2014 Европейского парламента и Совета Европейского Союза «О злоупотреблениях на рынке (Регламент о злоупотреблениях на рынке) и об отмене Директивы 2003/6/ЕС Европейского Парламента и Совета ЕС и Директив 2003/124/ЕС, 2003/125/ЕС и 2004/72/ЕС Европейской Комиссии» // СПС «КонсультантПлюс».

Таким образом, актуальное определение инсайдерской информации делает фактически невозможным в отдельных случаях ее незамедлительное раскрытие, исходя из режима защиты иных видов тайн.

Во-вторых, спорным является необходимость признания инсайдерской исключительно точной и конкретной информации. В правовой доктрине существуют мнения, что на фондовом рынке не всегда нужна точная и конкретная информация, так как порой для наступления последствий достаточно намека<sup>5</sup>. Как представляется, наличие этого признака неоправданно и чрезмерно ограничивает рассматриваемое понятие.

В европейском законодательстве характеристика «точности» инсайдерской информации формулируется не столь категорично: употребляется словосочетание «информация точного характера», что указывает на то, что термин «точности» не возводится в абсолюте, а предполагает существование какой-то смысловой грани, по достижении которой информацию можно считать информацией точного характера и при выполнении прочих условий трактовать ее как инсайдерскую. В пункте 2 ст. 7 MAR о злоупотреблениях на рынке приводится пояснение термина «информация точного характера», которое кратко можно сформулировать следующим образом: если информация в достаточной степени конкретна, чтобы, располагая ей, резонно ожидать наступления на ее основании определенных обстоятельств / событий, в результате которых цена финансового инструмента может измениться.

В-третьих, такой признак инсайдерской информации, как существенность влияния на цены финансовых инструментов, иностранной валюты и товаров, также является спорным. В отсутствие закрепления в законодательстве Российской Федерации порядка (либо подходов) оценки «существенности» влияния распространения информации на цены финансовых инструментов наличие такого признака может создавать трудности при обосновании позиции, в соответствии с которой та или иная информация должна считаться (или не считаться) инсайдерской в отсутствие установленных подходов, а также уменьшать доверие к корректности такой позиции.

Вместе с тем проблема дефиниции является не единственной в регулировании инсайдерской информации в России.

Вплоть до 3 августа 2018 г. перечень инсайдерской информации являлся исчерпывающим и устанавливал все возможные типы информации, которые требовалось считать инсайдерской. Отмена такого подхода,

<sup>5</sup> Клепицкий И.А. Инсайдерская информация и уголовный закон // Закон. 2011. № 9. С. 67–79 ; Федоров В.А. Закон об инсайте: аналитический комментарий // Российское предпринимательство. 2010. № 11. С. 88–92.

с одной стороны, позволила регулятору трактовать термин «инсайдерская информация» шире, с другой — должно было усилить режим безопасности чувствительной информации, относимой самими инсайдерами к инсайдерской информации.

Однако практика показала, что инсайдеры неохотно воспользовались правом дополнять исчерпывающий список при создании собственных перечней инсайдерской информации. Это во многом связано с тем, что инструкций или рекомендаций к составлению указанного списка нет, а ответственность за отсутствие информации, не включенной в исчерпывающий перечень, не предусмотрена. Анализ перечней инсайдерской информации таких лиц, публикуемых ими на официальных сайтах, показывает, что они обычно соответствуют составу исчерпывающего перечня Банка России и не содержат инициативных дополнений.

При этом, как представляется, развитие системы мягкого регулирования в противовес системе установления жестких требований, построение отношений регулятора и подконтрольных лиц на принципе доверия позволило бы значительно изменить формат отношений, а также стало бы стимулом для более ответственного, внимательно-го подхода к закреплению последними своих перечней инсайдерской информации.

Указанное подтверждается мировым опытом регулирования инсайдерской информации.

Понятий, аналогичных исчерпывающему и открытому перечням инсайдерской информации в российском законодательстве, в европейском законодательстве нет: инсайдерской информацией может считаться любая информация, соответствующая определению, данному в п. 1 ст. 7 MAR.

Согласно § 55 Закона Великобритании об уголовном правосудии 1993 г. инсайдерская информация — это информация, которая: 1) относится к определенным ценным бумагам или определенному эмитенту ценных бумаг, а не к ценным бумагам или эмитентам в целом; 2) является точной и конкретной; 3) не была публично раскрыта; 4) будучи публично раскрытой, оказала бы влияние на цену ценных бумаг, к которым относится. Какой-либо формализованный на уровне законодательства перечень инсайдерской информации отсутствует.

В Законе США о торговле ценными бумагами 1934 г. информация определяется как не являющаяся общедоступной информация об эмитенте и выпущенных им эмиссионных ценных бумагах, которая ставит лиц, обладающих такой информацией до момента ее публичного распространения, в преимущественное положение по отношению к другим участникам торгов. Однако в законодательстве США отсутствует

какой-либо перечень (индикативный открытый или императивный закрытый) информации, которая признается инсайдерской.

Таким образом, несмотря на ряд сходств между определением инсайдерской информации в российском и мировом законодательстве, концепция перечней инсайдерской информации характерна только для Федерального закона № 224-ФЗ.

Проблема закрепленного перечня инсайдерской информации, пусть и возможного к дополнению, имеет, как представляется, ряд недостатков.

Согласно Регламенту ЕС о злоупотреблениях на рынке существенной характеристикой инсайдерских сделок является несправедливое преимущество, полученное путем использования внутренней информации в ущерб третьим лицам, которым такая информация неизвестна, и, как следствие, нарушение целостности финансовых рынков и снижение доверия инвесторов. В том числе это касается случаев, когда менеджмент узнал о чем-то важном, что потенциально может повлиять на решения об инвестировании средств в данную компанию.

В отсутствие же расширения юридическим лицом-инсайдером перечня инсайдерской информации, предложенного нормативным актом Банка России, за пределами защиты Федерального закона № 224-ФЗ может остаться большой круг сведений, способных оказать влияние на стоимость финансовых инструментов, иностранной валюты и товаров.

Также необходимо отметить, что не для всех подконтрольных Банку России субъектов строго закрепленный перечень будет релевантным. К примеру, иностранные эмитенты, обращающиеся на российском рынке, имеют отличия от Российской Федерации в системе корпоративного управления, в связи с чем к ним неприменим в полной мере перечень инсайдерской информации, устанавливаемый регулятором. Соответствующие изъятия для иностранных эмитентов, являющихся иностранной организацией, эмиссионные ценные бумаги которой (ценные бумаги, удостоверяющие права в отношении представляемых эмиссионных ценных бумаг иностранной организации) допущены к организованным торгам в случае, предусмотренном пунктом 4 ст. 51.1 Федерального закона «О рынке ценных бумаг», были введены Банком России в 2021 г.<sup>6</sup> Вместе с тем вопрос необходимости соблюдения обязательных требова-

<sup>6</sup> Указание Банка России от 2 февраля 2021 г. № 5719-У «О внесении изменений в приложение к Указанию Банка России от 21 ноября 2019 года № 5326-У «О перечне инсайдерской информации юридических лиц, указанных в пунктах 1, 3, 4, 11 и 12 статьи 4 Федерального закона от 27 июля 2010 года № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации», а также о порядке и сроках ее раскрытия» // Официальный сайт Банка России. URL: <http://www.cbr.ru/>, 22.03.2021



ний Банка России в части содержания перечня инсайдерской информации иных иностранных эмитентов остается открытым.

Кроме того, как представляется, «мягкий» подход к составлению перечня инсайдерской информации участниками финансового рынка даст возможность составлять индикативные перечни, не закрепляя строгого списка конкретных документов, а отражая в таком перечне отдельные группы документов, объединенные общим признаком. Такой подход активно используется иностранными эмитентами, имеющими листинг, например, на американских биржах.

Отдельной частной проблемой является, по сути, дублирование для эмитентов режимов ряда информации: отдельные значимые сведения раскрываются эмитентами на рынке ценных бумаг в виде существенных фактов, та же информация подлежит раскрытию как инсайдерская.

Такое дублирование создает дополнительную административную нагрузку на эмитентов, воспринимаемую ими со значительной долей негатива.

Совершенно очевидно, что по истечении 10 лет со дня вступления в силу Федерального закона № 224-ФЗ можно сделать вывод о значительном скачке в развитии регулирования защиты инсайдерской информации в Российской Федерации. Вместе с тем, являясь молодым, российское законодательство об инсайте нуждается в развитии, а также сближении с иностранным законодательством.

### Литература

1. Гришаев С.П. Комментарий к Федеральному закону от 27 июля 2010 г. № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» / С.П. Гришаев // СПС «КонсультантПлюс». 2010.
2. Клепицкий И.А. Инсайдерская информация и уголовный закон / И.А. Клепицкий // Закон. 2011. № 9. С. 67–79.
3. Федоров В.А. Закон об инсайте: аналитический комментарий / В.А. Федоров // Российское предпринимательство. 2010. № 11. С. 88–92.

**Северин Виталий Андреевич,**  
профессор кафедры коммерческого права и основ правоведения  
Юридического факультета Московского государственного университета  
имени М.В. Ломоносова,  
руководитель магистерской программы  
«Информационные правоотношения в инновационной экономике»,  
доктор юридических наук  
*commercial@law.msu.ru*

## **ПРОЕКТ СЕТЕВОЙ МАГИСТЕРСКОЙ ПРОГРАММЫ ПОДГОТОВКИ ЮРИСТОВ НА МЕЖВУЗОВСКОЙ ПЛАТФОРМЕ**

Цифровизация общественных отношений формирует новую социальную, экономическую, политическую и правовую реальность, что требует совершенно иного подхода к вопросам переподготовки и обучения юридических кадров. В эпоху инноваций и использования новых информационных технологий нужен комплексный подход на основе междисциплинарных знаний. Опыт разработки и внедрения на юридическом факультете МГУ имени М.В. Ломоносова магистерской программы «Информационные правоотношения в инновационной экономике» может быть использован для открытия сетевой магистерской программы на межвузовской платформе. Автором подготовлен для обсуждения проект договора «О совместной образовательной программе МГУ имени М.В. Ломоносова и МГИМО МИД России» подготовки кадров юристов для цифровой экономики в условиях мирового информационного общества. В проекте договора автором сформулированы условия успешной реализации сетевой магистерской программы, вопросы научной специализации программы, порядок приема в магистратуру и проведение вступительного экзамена в соответствии с программами юридического факультета МГУ и МГИМО.

**Ключевые слова:** подготовка юристов, информационное общество, цифровая экономика, междисциплинарные знания, сетевая магистерская программа, проект договора на межвузовской платформе.

**Vitaly A. Severin**

Professor of the Department of Commercial Law and Fundamentals  
of Jurisprudence of the Faculty of Law of the Lomonosov Moscow State University  
Head of the Master's program "Information Legal Relations in the Innovative Economy"  
LL.D.

## **PROJECT OF A NETWORK MASTER'S PROGRAM FOR TRAINING LAWYERS ON AN INTERUNIVERSITY PLATFORM**

Training lawyers to work in an information society in an era of innovation requires a comprehensive approach based on interdisciplinary knowledge. The experience of developing

and implementing the master's program "Information Legal Relations in the Innovative Economy" at the Faculty of Law of the Lomonosov Moscow State University can be used to open a network master's program on an interuniversity platform. The author has prepared for discussion a draft agreement "On the joint educational program of the Moscow State University named after M. V. Lomonosov and MGIMO University of the Ministry of Foreign Affairs of Russia" training lawyers for the digital economy in the global information society. The program is competitive and will expand the opportunities to attract applicants for training. In the draft agreement, the author formulated the conditions for the successful implementation of the network master's program. It is necessary to solve questions about the scientific specialization of the program, the order of admission to the master's program and the conduct of the entrance exam, etc. in accordance with the programs of the Faculty of Law of Moscow State University and MGIMO.

**Keywords:** training of lawyers, information society, digital economy, interdisciplinary knowledge, network master's program, draft agreement on an inter-university platform.

Подготовка юристов нового поколения напрямую связана с реализацией программы «Цифровая экономика Российской Федерации». Курс государства на модернизацию экономики выявил пробел в знаниях юристов. Вузы по-прежнему готовят юристов для сырьевой экономики. Уровень юридической грамотности в информационной сфере достаточно низкий: юристы не получают должной подготовки для правового обеспечения цифровизации экономики, не способны грамотно сопровождать процессы НИОКР, слабо осведомлены в методах коммерциализации прав на результаты интеллектуальной деятельности, недостаточно владеют способами защиты информации<sup>1</sup>.

Подготовка юристов для работы в условиях информационного общества в эпоху инноваций требует комплексного подхода на основе междисциплинарных знаний. Сложность подготовки юристов для работы в информационной сфере объясняется неразработанностью государственных образовательных стандартов, учебных программ и курсов, когда действующая система базового образования не успевает адаптироваться к современным условиям формирования цифровой экономики. В 2016 г. на Юридическом факультете МГУ имени М.В. Ломоносова была открыта и реализуется магистерская программа «Информационные правоотношения в инновационной экономике» с целью подготовки юристов нового поколения в области правового обеспечения производства наукоемкой гражданской и военной продукции. В реализации программы принимает участие профессорско-преподавательский состав юридического факультета, экономического факультета, факультета вычислительной математики

<sup>1</sup> См.: Северин В.А. Перспективы подготовки юридических кадров в условиях развития инновационной экономики // Вестник Московского университета. Серия 11. Право. 2015. № 3. С. 66–85.

и кибернетики, Высшей школы государственного аудита, Военного учебного центра и Института проблем информационной безопасности МГУ (всего 18 преподавателей, включая 8 докторов наук). Опыт и творческий потенциал МГУ может быть использован в различных образовательных проектах с участием крупных организаций (корпораций, холдингов). Например, предлагается обсудить возможности совместного участия в подготовке магистров в области информационной безопасности по проекту «Совместная Образовательная программа МГУ имени М.В. Ломоносова и Университета Банка России» (далее — СОП) по направлению подготовки «Юриспруденция» на базе магистерской программы, реализуемой в МГУ, когда первый год студенты учатся в МГУ, а второй год (третий семестр) — в Университете Банка России. По результатам государственной итоговой аттестации обучающиеся получают документ о высшем образовании установленного образца, выдаваемый МГУ имени М.В. Ломоносова, и диплом о профессиональной переподготовке, выдаваемый Университетом Банка России. Наименование степени (квалификации), специальности, присуждаемой МГУ имени М.В. Ломоносова, — магистр по направлению «Юриспруденция», наименование новой квалификации, присваиваемой по итогам обучения в Университете Банка России, — «Мастер в области права информационной безопасности». Детальные положения, регулирующие взаимоотношения университетов-партнеров, будут определены договором.

Внедрение на юридическом факультете МГУ новой магистерской программы показывает, что для всестороннего понимания и сопровождения процесса превращения идеи в инновационный продукт, который выходит на мировой рынок, магистрантам нужны не только знания российского информационного, гражданского, административного, уголовного и других отраслей права<sup>2</sup>, но и зарубежного законодательства, судебной практики в области регулирования и защиты информации. Поэтому программа нуждается в совершенствовании структуры учебных курсов за счет введения новых дисциплин по вопросам международной информационной безопасности и научно-технологической политики.

Развитие магистерской программы, которая реализуется в МГУ, возможно на межвузовской платформе с участием других университетов и вузов. В частности, автором настоящей статьи подготовлен проект договора «О совместной образовательной программе МГУ имени М.В. Ломоносова и МГИМО МИД России» с целью упорядочить научное и практическое представление о совместной подготовке кадров юристов для цифровой экономики России в условиях развития мирового информационного общества. Базовая идея, заложенная в проекте договора, заключается в том, что-

<sup>2</sup> См.: Программа подготовки магистров «Информационные правоотношения в инновационной экономике»: учебное пособие. 3-е изд. исправл. и доп. / коллектив авторов; под общ. ред. и с предисловием В.А. Северина. М.: Издательский дом «Юр-ВАК», 2019. URL: <http://urvak.ru/books/>

бы к научным и профессиональным юридическим компетенциям, которые студенты получают в вузах, добавить способность практически создавать юридический бизнес и осуществлять правовое сопровождение организаций цифровой экономики в качестве адвокатов и практикующих юристов в России и за рубежом. В таком виде магистерская программа будет конкурентоспособной и расширит возможности по привлечению абитуриентов для обучения на программу.

Какие перспективы открытия межвузовской магистерской программы? Важно объединить усилия вузов с учетом их интересов в рамках сетевой межвузовской магистерской программы. Например, за основу можно взять программу, которая реализуется на юридическом факультете МГУ. Первый год студенты учатся на юридическом факультете МГУ, второй год — в Сетевом университете СНГ МГИМО. По окончании обучения выпускники получают два диплома магистра в области юриспруденции. Предлагается создать рабочую группу для проработки идеи внедрения в МГУ и МГИМО проекта сетевой магистерской программы «Информационные правоотношения в инновационной экономике» по направлению подготовки «Юриспруденция»; подготовки предложений для рассмотрения руководством МГУ и МГИМО о возможности выдачи выпускникам магистратуры двойного диплома МГУ и МГИМО по данной программе. При этом нужно исходить, что курсы / модули разных университетов должны взаимно дополнять друг друга в рамках концепции единой согласованной сетевой программы (то есть программа разделена на два модуля, каждый из которых реализуется только юридическим факультетом МГУ и МГИМО). Нужно решить вопросы о научной специализации программы, порядке приема в магистратуру и проведение вступительного испытания (экзамена) в соответствии с программами юридического факультета МГУ и МГИМО. Важным является разработка и согласование условий договора о партнерстве между юридическим факультетом МГУ и МГИМО о совместной подготовке магистров в рамках сетевой магистерской программы (проект договора прилагается).

## ДОГОВОР

*между*

Московским государственным университетом имени М.В. Ломоносова и Московским государственным институтом международных отношений (университет) Министерства иностранных дел Российской Федерации «О совместной образовательной программе МГУ имени М.В. Ломоносова и МГИМО МИД России»

*в Российской Федерации, г. Москва* по направлению подготовки 40.04.01 «Юриспруденция» уровня подготовки высшего образования: магистратуры с присвоением квалификации (степени) «магистр»;

в Российской Федерации, г. Москва по программе профессиональной переподготовки с присвоением новой квалификации «Мастер в области права международной информационной безопасности».

Основываясь на нормах законодательства Российской Федерации, разделяющего учебные заведения правом осуществлять сотрудничество в области высшего образования и преподавательской деятельности, в том числе посредством прямых договоров, заключенных образовательными организациями,

принимая во внимание, что высшее образование играет жизненно важную роль в улучшении взаимопонимания и в создании взаимного Доверия, желая предоставить студентам возможность получать свое образование в МГУ и МГИМО, прибегая к ресурсам обоих университетов,

считая, что совместная реализация и признание образовательных программ, учебных курсов представляет собой важную меру, направленную на удовлетворение потребностей общества в специалистах, обладающих фундаментальными знаниями и высоким творческим потенциалом, информированных о национальных и мировых достижениях,

руководствуясь российским законодательством о высшем образовании и принимая во внимание нормы международного права,

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования Московский государственный университет имени М.В. Ломоносова (Россия, Москва) в лице Ректора и Федеральное государственное автономное образовательное учреждение высшего образования Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации (Россия, Москва) в лице Ректора, также именуемые в дальнейшем Сторонами, заключили настоящий Договор о нижеследующем:

## 1. Основные понятия и термины

1.1. *Университеты-партнеры, или Стороны* — университеты, заключающие настоящий Договор, а именно Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Московский государственный университет имени МВ. Ломоносова» и «Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации».

1.2. *Квалификация* — уровень знаний, умений, навыков и компетенции, характеризующий подготовленность к выполнению определенного вида профессиональной деятельности.

1.3. *Федеральный государственный образовательный стандарт высшего образования* — совокупность обязательных требований к образованию определенного уровня и (или) к профессии, специальности и направлению подготовки, утвержденных федеральным органом исполнительной власти

Российской Федерации, осуществляющим функции по выработке государственной политики и нормативно-правовому регулированию в сфере образования. ФГОС ВО по направлению подготовки магистров «Юриспруденция», утвержденный приказом Министерства образования и науки Российской Федерации от 1 декабря 2010 г. № 1511.

1.4. *Образовательный стандарт МГУ имени М.В. Ломоносова* — образовательный стандарт МГУ, представляющий собой совокупность требований, обязательных при реализации основных образовательных программ высшего образования — программ магистратуры в МГУ имени М.В. Ломоносова для подготовки магистров по направлению «Юриспруденция». Образовательный стандарт, самостоятельно устанавливаемый МГУ для реализуемых образовательных программ высшего образования по направлению подготовки «Юриспруденция» утвержденный приказом МГУ «Об утверждении образовательных стандартов МГУ» от 22 июля 2011 г. № 729 (пункт 2) и приказом МГУ «Об утверждении и изменении образовательных стандартов МГУ от 27 апреля 2012 г.

1.5. *Образовательная программа* — комплекс основных характеристик образования (объем, содержание, планируемые результаты), организационно-педагогических условий и в случаях, предусмотренных Федеральным законом от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», форм аттестации, который представлен в виде учебного плана, календарного учебного графика, рабочих программ учебных предметов, курсов, дисциплин (модулей), иных компонентов, а также оценочных и методических материалов.

1.6. *Профессиональное образование* — вид образования, который направлен на приобретение обучающимися в процессе освоения основных профессиональных образовательных программ знаний, умений, навыков и формирование компетенции определенных уровня и объема, позволяющих вести профессиональную деятельность в определенной сфере и (или) выполнять работу по конкретным профессии или специальности.

*Дополнительное профессиональное образование* — вид образования, который направлен на удовлетворение образовательных и профессиональных потребностей, профессиональное развитие человека, обеспечение соответствия его квалификации меняющимся условиям профессиональной деятельности и социальной среды.

1.7. *Обучающийся* — физическое лицо, осваивающее образовательную программу.

1.8. *Обучающийся с ограниченными возможностями здоровья* — физическое лицо, имеющее недостатки в физическом и (или) психологическом развитии, подтвержденные психолого-медико-педагогической комиссией и препятствующие получению образования без создания специальных условий.

1.9. *Образовательная деятельность* — деятельность по реализации образовательных программ.

1.10. *Научно-педагогический работник* — физическое лицо, которое стоит в трудовых или в гражданско-правовых отношениях с организацией, осуществляющей образовательную деятельность, и выполняет обязанности по обучению, воспитанию обучающихся и (или) организации образовательной деятельности.

1.11. *Учебный план* — документ, который определяет перечень, трудоемкость, последовательность и распределение по периодам обучения учебных предметов, курсов, дисциплин (модулей), практики, иных видов учебной деятельности и, если иное не установлено Федеральным законом от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», формы промежуточной аттестации обучающихся,

1.12. *Индивидуальный учебный план* — учебный план, обеспечивающий освоение образовательной программы на основе индивидуализации ее содержания с учетом особенностей и образовательных потребностей конкретного обучающегося.

1.13. *Практика* — вид учебной деятельности, направленной на формирование, закрепление, развитие практических навыков и компетенции в процессе выполнения определенных видов работ, связанных с будущей профессиональной деятельностью.

1.14. *Направленность (профиль) образования* — ориентация образовательной программы на конкретные области знания и (или) виды деятельности, определяющая ее предметно-тематическое содержание, преобладающие виды учебной деятельности обучающегося и требования к результатам освоения образовательной программы.

1.15. *Средства обучения* — приборы, оборудование, включая спортивное оборудование и инвентарь, инструменты, учебно-наглядные пособия, компьютеры, информационно-телекоммуникационные сети, аппаратно-программные и аудиовизуальные средства, печатные и электронные образовательные и информационные ресурсы и иные материальные объекты, необходимые для организации образовательной деятельности.

1.16. *Инклюзивное образование* — обеспечение равного доступа к образованию для всех обучающихся с учетом разнообразия особых образовательных потребностей и индивидуальных возможностей.

1.17. *Адаптированная образовательная программа* — образовательная программа, адаптированная для обучения лиц с ограниченными возможностями здоровья с учетом особенностей их психофизического развития, индивидуальных возможностей и при необходимости обеспечивающая коррекцию нарушений развития и социальную адаптацию указанных лиц.

1.18. *Качество образования* — комплексная характеристика образовательной деятельности и подготовки обучающегося, выражающая степень их соответствия федеральным государственным образовательным стандартам, образовательным стандартам, федеральным государственным требованиям и (или) потребностям физического или юридического лица, в



интересах которого осуществляется образовательная деятельность, в том числе степень достижения планируемых результатов образовательной программы.

1.19. *Совместная Образовательная программа МГУ имени М.В. Ломоносова и МГИМО МИД России (далее — СОП)* — образовательная программа, совместно организуемая и реализуемая МГУ и МГИМО, в рамках которой обучающиеся учатся в МГУ и МГИМО, и по результатам успешного освоения которой предусматривается получение обучающимися документов об образовании каждого из Университетов-партнеров — Сторон настоящего Договора.

1.20. *Кандидат на участие в СОП* — студент МГУ, подавший заявление на обучение по совместной образовательной программе в МГИМО, а также слушатель МГИМО, подавший заявление на обучение по совместной образовательной программе в МГУ.

1.21. *Университет-партнер А* — ФГБОУ ВО «МГУ имени М.В. Ломоносова».

1.22. *Университет-партнер В* — ФГАОУ ВО «МГИМО МИД России».

1.23. *Резидентная часть учебного плана* — часть учебного плана, реализуемая в ФГБОУ ВО «МГУ имени МВ. Ломоносова».

1.24. *Нерезидентная часть учебного плана* — часть учебного плана, реализуемая в ФГАОУ ВО «МГИМО МИД России».

## 2. Предмет Договора

2.1. Настоящий Договор регулирует общие вопросы сотрудничества Университетов-партнеров при реализации совместной образовательной программы магистратуры по направлению «Юриспруденция», обеспечивающей возможность освоения обучающимися образовательной программы с использованием ресурсов ФГБОУ ВО «МГУ имени М.В. Ломоносова» и ФГАОУ ВО «МГИМО МИД России».

2.2. Детальные положения, регулирующие взаимоотношения Университетов-партнеров в различных сферах, будут определены в приложениях и дополнениях к настоящему Договору, являющихся его неотъемлемыми частями.

## 3. Правовое регулирование

3.1. При осуществлении образовательной деятельности по СОП каждый Университет-партнер руководствуется:

- действующим законодательством Российской Федерации;
- настоящим Договором;
- нормативными документами (локальными актами) Университетов-партнеров по вопросам образовательной, административной и иной деятельности.

#### 4. Структура и содержание СОП

4.1. Содержание СОП определяется рабочим учебным планом, согласованным представителями Университетов-партнеров, а также утвержденными в установленном порядке учебными планами Университетов-партнеров, которые являются неотъемлемой частью настоящего Договора.

4.2. Содержание рабочего плана СОП определяется протоколами соответствия учебного плана, являющимися неотъемлемыми частями настоящего Договора.

4.3. Срок освоения СОП подготовки магистров составляет два года и состоит из трех этапов. Реализация СОП на первом этапе (первый и второй семестры обучения) осуществляется в МГУ, на втором этапе (третий семестр обучения) в МГИМО, на заключительном этапе (четвертый семестр обучения) в МГУ.

4.4. Обучение студентов МГУ в МГИМО и слушателей МГИМО в МГУ осуществляется с использованием протоколов соответствия.

4.5. При направлении в МГИМО для обучающихся по СОП подготовки магистров используются следующие Протоколы соответствия учебного плана: третий семестр обучения: Приложение № 2.

4.6. Содержание Протоколов соответствия учебного плана может меняться по взаимному соглашению сторон в связи с изменением утвержденных в установленном порядке учебных планов, а также с учетом возможных потребностей дальнейшей модернизации и совершенствования учебного процесса, осуществляемого в рамках СОП.

4.7. Изменения протоколов соответствия учебных планов утверждаются в форме приложений к настоящему Договору.

#### 5. Управление СОП

5.1. В целях координации деятельности по созданию и реализации СОП Университеты-партнеры формируют Рабочую группу по реализации СОП ФГБОУ ВО «МГУ имени М.В. Ломоносова» и ФГАОУ ВО «МГИМО МИД России», именуемую в дальнейшем «Рабочая группа».

5.2. Рабочая группа состоит из представителей Университетов-партнеров — участников данной программы. Персональный состав Рабочей группы утверждается руководителями Университетов-партнеров.

5.3. В компетенцию Рабочей группы входит решение всех методических и организационных вопросов реализации СОП. Структурные подразделения Университетов-партнеров, осуществляющие реализацию СОП, организуют информационное и учебно-методическое обеспечение обучающихся в рамках СОП.

5.4. Представители Университетов-партнеров, входящие в состав Рабочей группы, ответственны за отбор кандидатов на обучение по СОП, за организационные и иные вопросы реализации СОП.

5.5. В случае если для решения какого-либо вопроса требуется согласие руководящих органов Университетов-партнеров, Рабочая группа вправе направлять в соответствующие органы управления Университетов предложения для их дальнейшего рассмотрения и утверждения.

5.6. Каждое решение Рабочей группы оформляется соответствующим протоколом в двух экземплярах и подписываются соруководителями СОП.

## **6. Зачисление студентов МГУ на СОП**

6.1. Обучающиеся в МГУ, изъявившие желание обучаться по СОП, направляются в МГИМО МИД России на включенное обучение в соответствии с порядком, установленным Положением МГУ от 17 июня 2013 года «О порядке направления студентов (бакалавров, магистров, специалистов) на включенное обучение».

6.2. Для обучения по СОП студент МГУ подает в Университет-партнер А заявление с указанием Университета-партнера В (Приложение № 1). Форма заявления и перечень документов, необходимых для поступления на СОП, утверждаются Университетами-партнерами.

6.3. Университет-партнер А рассматривает заявление и в случае готовности принять кандидата на участие в СОП на обучение передает комплект документов в Университет-партнер В, указанный в заявлении, для согласования кандидатуры.

6.4. Зачисление кандидатов на участие в СОП на обучение в Университет-партнер В осуществляется путем издания отдельного приказа в порядке, установленном в Университете-партнере В.

6.5. При зачислении на обучение в Университете-партнере В на СОП может взиматься плата за оформление документов и иные услуги, размер которой устанавливается Университетом-партнером В самостоятельно. Кандидат на участие в СОП должен быть уведомлен о размере и сроках указанной платы в каждом из Университетов-партнеров В при подаче заявления о приеме.

6.6. Кандидат на участие в СОП при зачислении должен быть ознакомлен Университетами-партнерами А и В с документами программы, в том числе с настоящим Договором и приложениями к нему.

6.7. Обучающийся заключает отдельный договор на оказание платных образовательных услуг с Университетом-партнером В.

6.8. С обучающимся в Университете-партнере А по договору на оказание платных образовательных услуг с оплатой стоимости обучения, заключается дополнительное соглашение к этому договору, предусматривающее изменения в порядке оказания и оплаты образовательных услуг. Не допускается взимание платы за обучение по данному договору в Университете-партнере А во время нахождения студента на обучении в Университете-партнере В.

## 7. Статус (права и обязанности) обучающихся

7.1. Обучающимся предоставляются, в частности, академические права на:

— обучение по индивидуальному учебному плану в пределах осваиваемой СОП в порядке, установленном локальными нормативными актами Университетов-партнеров;

— освоение наряду с учебными предметами, курсами, дисциплинами (модулями) по осваиваемой СОП других учебных предметов, курсов, дисциплин (модулей), преподаваемых в Университетах-партнерах, осуществляющих образовательную деятельность, в установленном порядке;

— каникулы — плановые перерывы при получении образования для отдыха и иных социальных целей в соответствии с законодательством об образовании и календарным учебным графиком;

— пользование библиотечно-информационными ресурсами, учебной, научной базой Университетов-партнеров;

— пользование в порядке, установленном локальными нормативными актами, лечебно-оздоровительной инфраструктурой, социальными объектами, объектами культуры и объектами спорта Университетов-партнеров;

— развитие своих творческих способностей и интересов, включая участие в конкурсах, олимпиадах, выставках, смотрах, физкультурных мероприятиях, спортивных мероприятиях, в том числе в официальных спортивных соревнованиях, и других массовых мероприятиях;

— участие в соответствии с действующим законодательством в научно-исследовательской, научно-технической, экспериментальной и инновационной деятельности, осуществляемой Университетами-партнерами, под руководством научно-педагогических работников Университетов-партнеров;

— иные академические права, предусмотренные Федеральным законом от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации», иными нормативными правовыми актами Российской Федерации, локальными нормативными актами Университетов-партнеров.

7.2. Обучающиеся имеют право на посещение по своему выбору мероприятий, которые проводятся в Университетах-партнерах, реализующих СОП, и не предусмотрены учебным планом, в порядке, установленном локальными нормативными актами. Привлечение обучающихся без их согласия и несовершеннолетних обучающихся без согласия их родителей (законных представителей) к труду, не предусмотренному СОП, не допускается.

7.3. В процессе реализации СОП при обучении в одном из Университетов-партнеров обучающиеся пользуются всеми правами, установленными для обучающихся данного Университета.

7.4. В течение срока получения образования по СОП обучающиеся обязаны выполнять все требования Уставов Университетов-партнеров, тре-

бования, связанные с выполнением настоящего Договора, включая посещение занятий и других мероприятий в рамках СОП. За нарушения требований каждого Университета-партнера к обучающимся могут быть применены меры дисциплинарного воздействия в установленном порядке.

### **8. Условия и порядок осуществления образовательной деятельности по СОП**

8.1. Уровень квалификации научно-педагогических работников, позволяющий им осуществлять обучение, воспитание и организацию образовательной деятельности, определяется по законодательству Российской Федерации и подтверждается соответствующими документами.

8.2. При реализации СОП могут применяться электронное обучение и дистанционные образовательные технологии, обеспечивающие удаленный доступ к оборудованию, программным средам, образовательному контенту и взаимодействие между участниками образовательного процесса. При обучении инвалидов и лиц с ограниченными возможностями здоровья дистанционные образовательные технологии должны предусматривать возможность приема-передачи информации в доступных для них формах.

8.3. Периоды обучения и академическая аттестация, пройденные обучающимися в рамках СОП в одном из Университетов-партнеров, взаимно признаются другим Университетом-партнером, подписавшими настоящий Договор.

8.4. Контроль качества обучения по СОП осуществляется уполномоченными структурными подразделениями Университетов-партнеров. Внешний контроль качества обучения по совместной образовательной программе, осуществляемого одним из Университетов-партнеров на каждом этапе реализации СОП, может осуществляться представителями любого Университета-партнера, Рабочей группы или внешними экспертами, привлеченными Рабочей группой и/или по заявлению и за счет другого Университета-партнера.

8.5. Государственная итоговая аттестация обучающихся, в том числе защита выпускной квалификационной работы, осуществляется в очной форме в ФГБОУ ВО «МГУ имени М.В. Ломоносова».

8.6. По результатам государственной итоговой аттестации обучающиеся, успешно освоившие СОП, получают документ о высшем образовании установленного образца, выдаваемый в ФГБОУ ВО «МГУ имени М.В. Ломоносова», и диплом о профессиональной переподготовке, выдаваемый в ФГАОУ ВО «МГИМО МИД России». Наименование степени (квалификации), специальности присуждаемой ФГБОУ ВО «МГУ имени М.В. Ломоносова» — магистр по направлению «Юриспруденция», наименование новой квалификации, присваиваемой по итогам обучения в ФГАОУ ВО «МГИМО МИД России» — «Мастер в области права международной информационной безопасности».

8.7. Характер и объем ресурсов, используемых ФГБОУ ВО «МГУ имени М.В. Ломоносова» для реализации СОП:

— используемые по согласованному расписанию помещения юридического факультета, в том числе в части эксплуатационных расходов: электроэнергия, отопление, водоснабжение и т.п.,

— административно-организационные мероприятия по информированию абитуриентов и обучающихся по СОП и их родителей (законных представителей) об образовательной деятельности ФГБОУ ВО «МГУ имени М.В. Ломоносова» и ФГАОУ ВО «МГИМО МИД России» по настоящему Договору;

— организация и учебно-методическое обеспечение образовательного процесса.

Характер и объем ресурсов, используемых ФГАОУ ВО «МГИМО МИД России» для реализации СОП:

— используемые по согласованному расписанию помещения, в том числе в части эксплуатационных расходов: электроэнергия, отопление, водоснабжение и т.п.;

— административно-организационные мероприятия по информированию абитуриентов и обучающихся по СОП и их родителей (законных представителей) об образовательной деятельности ФГБОУ ВО «МГУ имени М.В. Ломоносова» и ФГАОУ ВО «МГИМО МИД России» по настоящему Договору;

— организация и учебно-методическое обеспечение образовательного процесса.

## **9. Обязанности Сторон по организации учебного процесса**

9.1. ФГБОУ ВО «МГУ имени М.В. Ломоносова» обязуется:

— оказывать высококачественные образовательные услуги в соответствии с согласованной Сторонами СОП;

— обеспечивать образовательный процесс с привлечением высококвалифицированных кадров;

— осуществлять учебно-методическое обеспечение СОП;

— обеспечивать обучающихся необходимой учебной литературой;

— консультировать научно-педагогических работников об особенностях и специфике работы с обучающимися по СОП;

— по итогам успешного прохождения государственной итоговой аттестации выдать обучающемуся документ о высшем образовании установленного образца ФГБОУ ВО «МГУ имени М.В. Ломоносова» — магистр по направлению «Юриспруденция»;

— обеспечить информационную поддержку СОП, том числе размещение соответствующей информации на официальном интернет-сайте ФГБОУ ВО «МГУ имени М.В. Ломоносова» в форме, доступной для обучающихся и сотрудников ФГАОУ ВО «МГИМО МИД России»;

— обеспечить комфортные и безопасные условия для обучающихся и научно-педагогических работников, привлекаемых к реализации СОП.

9.2. ФГАОУ ВО «МГИМО МИД России» обязуется:

— оказывать высококачественные образовательные услуги в соответствии с согласованной Сторонами СОП;

— обеспечивать образовательный процесс с привлечением высококвалифицированных кадров;

— осуществлять учебно-методическое обеспечение СОП;

— обеспечивать обучающихся необходимой учебной литературой;

— по итогам успешного прохождения СОП выдать обучающемуся диплом о профессиональной переподготовке ФГАОУ ВО «МГИМО МИД России» («Мастер в области права международной информационной безопасности»);

— консультировать научно-педагогических работников об особенностях и специфике работы с обучающимися по СОП;

— обеспечить информационную поддержку СОП, в том числе размещение соответствующей информации на официальном интернет-сайте ФГАОУ ВО «МГИМО МИД России» в форме, доступной для обучающихся ФГБОУ ВО «МГУ имени М.В. Ломоносова»;

— обеспечить комфортные и безопасные условия для обучающихся, привлекаемых к реализации СОП.

9.3. При реализации включенного обучения инвалидов и лиц с ограниченными возможностями здоровья Университеты-партнеры предусматривают специализированные адаптационные модули (дисциплины) в рамках той части СОП, которая формируется участниками образовательных отношений.

9.4. Обучающиеся инвалиды и лица с ограниченными возможностями здоровья обеспечиваются печатными и электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

9.5. Научно-педагогические работники Университетов-партнеров должны быть ознакомлены с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья и учитывать их при организации образовательного процесса по СОП.

## **10. Источники и порядок финансирования СОП**

10.1. Обучение может финансироваться за счет:

— средств фондов поддержки и развития образования;

— личных средств обучающихся, их родителей и спонсоров;

— иных источников средств, не противоречащих законодательству Российской Федерации.

10.2. Каждый Университет-партнер самостоятельно в установленном порядке определяет стоимость обучения для приема обучающихся в следу-

ющем учебном году по СОП и доводит ее в установленном порядке до сведения руководства другого Университета-партнера.

10.3. Каждый Университет-партнер самостоятельно в установленном порядке утверждает расценки на оплату труда научно-педагогических работников, привлекаемых к реализации СОП.

10.4. Плата за обучение по СОП производится обучающимся по отдельному договору с каждым Университетом-партнером по графику, определенному в договоре с каждым Университетом-партнером.

10.5. При использовании общежитий/кампусов Университетов-партнеров стоимость проживания для обучающихся по СОП рассчитывается на основе общих тарифов, установленных в Университете-партнере.

10.6. Взаимные расчеты, связанные с осуществлением образовательных программ, являющихся предметом настоящего Договора, между Сторонами не производятся.

10.7. Никакие положения настоящего Договора не означают обязательств Сторон предоставлять друг другу услуги на возмездной и (или) безвозмездной основе.

## **11. Срок действия Договора, порядок его изменения и прекращения**

11.1. Настоящий Договор действителен в течение 5 (пяти) лет с момента его подписания.

11.2. По истечении срока действия настоящего Договора он может быть пролонгирован на следующий пятилетний срок посредством заключения дополнительного протокола к настоящему Договору. В случае прекращения действия настоящего Договора Университеты-партнеры обязуются полностью выполнить свои обязательства по отношению к обучающимся, принятым на обучение по СОП до момента его расторжения.

11.3. Договор может быть расторгнут по инициативе любого из Университетов-партнеров. В этом случае Университет-партнер — инициатор расторжения Договора должен предупредить другой Университет-партнер о расторжении соглашения не менее чем за 6 (шесть) месяцев до начала набора обучающихся на СОП и при этом завершить обучение по оформленным договорам с обучающимися.

11.4. Все изменения, дополнения к настоящему Договору и/или его положениям, принимаются Университетами-партнерами совместно.

11.5. Все изменения и дополнения к настоящему соглашению являются действительными, если они внесены в письменной форме и подписаны уполномоченными представителями Сторон.

## **12. Иные условия**

12.1. Все споры и разногласия, которые могут возникнуть из настоящего соглашения или в связи с ним, будут решаться путем переговоров между Университетами-партнерами.



12.2. Информация, полученная в ходе реализации настоящего соглашения и признанная сторонами конфиденциальной, не подлежит разглашению или передаче третьим лицам.

12.3. Договор составлен в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждого из Университетов-партнеров. Все экземпляры имеют равную юридическую силу.

Ректор  
МГУ имени М.В. Ломоносова МГИМО МИД России

---

*Приложение № 1*

Образец заявления

Проректору — начальнику Управления  
международного сотрудничества МГУ имени  
М.В. Ломоносова

---

студента \_\_\_ курса магистратуры очно-за-  
очного (вечернего) отделения Юридическо-  
го факультета МГУ  
ФИО

**Заявление**

Прошу Вас рассмотреть мою кандидатуру при отборе студентов для участия в совместной образовательной программе МГУ имени М.В. Ломоносова и Московского государственного института международных отношений (университет) МИД России на период с 20\_\_\_ по 20\_\_\_ г.

С содержанием и условиями участия в совместной образовательной программе ознакомлен и согласен.

Дата Подпись

Согласовано:

Управление академической политики и организации учебного процесса МГУ

«\_\_» \_\_\_\_\_ 20\_\_ года

**ПРОТОКОЛ соответствия учебного плана (учебных дисциплин) для направления студента МГУ на включенное обучение в вуз-партнер в осеннем семестре 20\_/20\_ уч. года**

Ф.И.О. студента

Факультет, курс — Юридический факультет, 2 курс (3 семестр)

Направление подготовки (специальность) в МГУ — магистр юриспруденции

Профиль подготовки — гражданско-правовой

Период включенного обучения — 01.09.20\_\_ «\_\_» \_\_\_\_\_ 20\_\_ года

Вуз-партнер — ФГАОУ ВО «МГИМО МИД России»

Номер и дата соглашения с вузом-партнером — Соглашение №\_\_ от «\_\_» \_\_\_\_\_ 20\_\_ года. Факультет в вузе-партнере — юридический факультет ФГБОУ ВО «МГУ имени М.В. Ломоносова»

Направление подготовки (квалификация) в вузе-партнере — мастер в области права международной информационной безопасности

Контактная информация принимающей стороны —

	Список всех дисциплин учебного плана МГУ на период включенного обучения	Зачетные единицы / общее количество академических часов (в том числе аудиторных) с указанием формы отчетности (зачет / экзамен)	Список дисциплин, предлагаемых вузом-партнером, соответствие которых учебному плану МГУ признается факультетом как соответствующий дисциплинам учебного плана МГУ	Зачетные единицы / общее количество академических часов (в том числе аудиторных) с указанием формы отчетности (зачет / экзамен)
1	Иностранный язык в правоведении	4/144 (64) экзамен	Иностранный язык в правоведении	4/144 (64) экзамен
2	История отечественного правоведения	2/72 (48) зачет	История отечественного правоведения	2/72 (48) зачет
3	Интеллектуальная собственность в инновационной экономике (на английском языке)	2/72 (32) экзамен	Интеллектуальная собственность в инновационной экономике (на английском языке)	2/72 (32) экзамен

4	Правовое обеспечение безопасности использования ИКТ в инновационных процессах (на английском языке)	2/72 (32) экзамен	Правовое обеспечение безопасности использования ИКТ в инновационных процессах (на английском языке)	2/72 (16) экзамен
5	Защита интересов государства в информационной сфере и инновационная экономика	2/72 (16) зачет	Защита интересов государства в информационной сфере и инновационная экономика	2/72 (16) зачет
6	Научно-исследовательский семинар	1/36 (16) зачет	Научно-исследовательский семинар	1/36 (16) зачет
7	Дисциплина из вариативной части учебного плана по выбору студента	2/72 (32) зачет	Дисциплина из вариативной части учебного плана по выбору студента	2/72 (32) зачет
8	Дисциплина из вариативной части учебного плана по выбору студента	3/108 (16) зачет	Дисциплина из вариативной части учебного плана по выбору студента	3/108 (16) зачет
9	Дисциплина из вариативной части учебного плана по выбору студента	2/72 (16) зачет	Дисциплина из вариативной части учебного плана по выбору студента	2/72 (16) зачет
10	Дисциплина из вариативной части учебного плана по выбору студента	2/72 (16) зачет	Дисциплина из вариативной части учебного плана по выбору студента	2/72 (16) зачет
11	Дисциплина из вариативной части учебного плана по выбору студента	2/72 (16) зачет	Дисциплина из вариативной части учебного плана по выбору студента	2/72 (16) зачет
	итого	25/ 900 (288)	итого	25/ 900 (288)
	ИТОГО соответствует	25/900 (288)		

Факультет предлагает признать соответствие указанных дисциплин дисциплинам учебного плана МГУ.

Итоговая государственная аттестация студента будет осуществлена в очной форме в МГУ.

По завершении включенного обучения студент обязан сдать академическую разницу в соответствии с отдельно утвержденным индивидуальным графиком по следующим дисциплинам в рамках учебного плана:

	<b>Список дисциплин учебного плана МГУ на период включенного обучения</b>	<b>Зачетные единицы / общее количество академических часов (в том числе аудиторных) с указанием формы отчетности (зачет / экзамен)</b>
1	Дисциплина из вариативной части учебного плана по выбору студента	2/72 (16) зачет
2	Дисциплина из вариативной части учебного плана по выбору студента	2/72 (16) зачет
3	Дисциплина из вариативной части учебного плана по выбору студента	2/72 (16) зачет
4	Дисциплина из вариативной части учебного плана по выбору студента	3/108 (16) зачет
	итого	9/324 (64)

Факультетом предусмотрены следующие меры для обеспечения освоения студентом указанных дисциплин:

1. Указанные дисциплины будут сланы студентом в соответствии с индивидуальным графиком обучения.

Во время включенного обучения планируется также освоение студентом следующих дисциплин вуза-партнера за рамками учебного плана МГУ:

	<b>Список дисциплин в вузе-партнере, освоение которых планируется за период включенного обучения за рамками учебного плана МГУ</b>	<b>Зачетные единицы / общее количество академических часов (в том числе аудиторных) с указанием формы отчетности (зачет/экзамен)</b>
1	Дисциплина из вариативной части учебного плана по выбору студента	2/72 (16) зачет
2	Дисциплина из вариативной части учебного плана по выбору студента	2/72 (16) зачет
	итого	4/144 (32)

#### Соответствие системы оценок в МГУ и в МГИМО

<b>Оценка в соответствии с учебными планами МГУ</b>	<b>Оценка в соответствии с учебными планами вуза-партнера</b>
Отлично	9, 10 баллов
Хорошо	6, 7, 8 баллов
Удовлетворительно	4, 5 баллов
Неудовлетворительно	1, 2 балла
Зачтено	свыше 3 баллов
Не зачтено	1, 2 балла

Декан юридического факультета \_\_\_\_\_

Студент \_\_\_\_\_

Дата

Приложения:

копия учебного плана вуза-партнера;  
копия документа о системе оценок, принятой в вузе-партнере; учебная карточка студента, распечатанная из АИС «Студент» учебного комплекса МГУ.

**Литература**

1. Алпатова И. Число IT-специалистов увеличится в три раза к 2024 году / И. Алпатова // Российская газета. 2020. 19 октября. URL: <https://rg.ru/2020/10/19/chislo-it-specialistov-uvelichitsia-v-tri-raza-k-2024-godu.html>
2. Зорькин В. Право в цифровом мире / В. Зорькин // Российская газета — Столичный выпуск. 2018. 29 мая ; Его же. Право будущего в эпоху цифр / В. Зорькин // Российская газета. 2020. 15 апреля. URL: <https://rg.ru/author-Valerij-Zorkin/>
3. Концепция Информационного кодекса Российской Федерации / ред. И.Л. Бачило. Москва : Канон-Плюс, 2014. 191 с.
4. Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» : утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 4 июня 2019 г. № 7 // URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_328854/](http://www.consultant.ru/document/cons_doc_LAW_328854/)
5. Программа подготовки магистров «Информационные правоотношения в инновационной экономике» : учебное пособие. 3-е изд., исправл. и доп. / коллектив авторов ; под общ. ред. и с предисловием В.А. Северина. Москва : Издательский дом «Юр-ВАК», 2019. 224 с. URL: <http://urvak.ru/books/>
6. Северин В.А. Перспективы подготовки юридических кадров в условиях развития инновационной экономики / В.А. Северин // Вестник Московского университета. Серия 11. Право. 2015. № 3.
7. Северин В.А. Внедрение магистерской программы для подготовки юристов нового поколения в МГУ имени М.В. Ломоносова / В.А. Северин // Право интеллектуальной собственности. 2017. № 1.
8. Урсул А.Д. Информация и глобальные процессы: междисциплинарные исследования / А.Д. Урсул // Знание. Понимание. Умение. 2013. № 3.
9. Ушакова С.Е. VIII Международный форум «Инновационное развитие через рынок интеллектуальной собственности» / С.Е. Ушакова., О.Л. Сергеева // Управление наукой и наукометрия. 2016. № 3. URL: <https://cyberleninka.ru/article/n/viii-mezhdunarodnyy-forum-innovatsionnoe-razvitie-cherez-rynok-intellektualnoy-sobstvennosti> (дата обращения: 09.09.2021).
10. Фомин И.Н. Влияние информации на ускорение развития общества / И.Н. Фомин // Технические науки — от теории к практике. 2012. № 14. URL: <https://cyberleninka.ru/article/n/vliyanie-informatsii-na-uskorenie-razvitiya-obschestva> (дата обращения: 09.09.2021).

## МАГИСТЕРСКАЯ ПРОГРАММА «ИНФОРМАЦИОННЫЕ ПРАВООТНОШЕНИЯ В ИННОВАЦИОННОЙ ЭКОНОМИКЕ»

<b>Профиль:</b>	Гражданско-правовой	Руководитель программы: доктор юридических наук, профессор кафедры коммерческого права и основ правоведения <b>Северин Виталий Андреевич</b>
<b>Наименование:</b>	Информационные правоотношения в инновационной экономике	
<b>Продолжительность обучения:</b>	2 года	
<b>Язык:</b>	русский	
<b>Формат обучения: Набор:</b>	очно-заочная (вечерняя) 2021–2023 уч. год	

### О ПРОГРАММЕ

Магистерская программа «Информационные правоотношения в инновационной экономике» является межкафедральной, носит междисциплинарный характер и реализуется силами профессорско-преподавательского состава юридического факультета с участием 4 факультетов и Института проблем информационной безопасности МГУ.

Программа направлена на подготовку юристов, обладающих современными знаниями и практическими навыками в информационной сфере для работы в государственных органах власти, в организациях, осуществляющих сбор, формирование, распространение и использование информации, занимающихся созданием и применением информационных систем, средств и механизмов информационной безопасности, в научно-исследовательских учреждениях РАН и вузах, ведущих подготовку по информационно-правовой специализации, в юридических фирмах, осуществляющих правовое сопровождение инновационного бизнеса.

#### Учебные курсы читают преподаватели МГУ имени М.В. Ломоносова:

✓ **Юридического факультета** (профессор, д.ю.н. **Северин В.А.**, профессор, д.ю.н. **Варламова А.Н.**, профессор, д.ю.н., заслуженный профессор Московского университета **Зенин И.А.**, профессор, д.ю.н. **Крылова Н.Е.**, доцент, к.ю.н. **Леонова Г.Б.**, доцент, к.ю.н. **Филатова М.А.**, доцент, к.ю.н. **Филиппова С.Ю.**);

✓ **Экономического факультета** (зам. декана по межфакультетскому взаимодействию и инновационной деятельности, зав. кафедрой, почетный работник высшего профессионального образования РФ, д.э.н., проф. **Иващенко Н.П.** и преподаватели кафедры экономики инноваций);

✓ **Факультета вычислительной математики и кибернетики, кафедра информационной безопасности** (директор центра современных информационных технологий, доцент, к.ф.-м.н. **Чижов И.В.**, доцент, к.ф.-м.н. **Применко Э.А.**);

- ✓ **Высшей школы государственного аудита (факультет)** (доцент, к.э.н. **Анищенко Е.В.**, доцент, к.э.н. **Боканов А.А.**, доцент, к.ю.н. **Семенкина Н.А.**);
- ✓ **Военного учебного центра** (доцент **Борисов М.А.**);
- ✓ **Института проблем информационной безопасности** (заместитель директора, заслуженный деятель науки РФ, д.ю.н., д.т.н., проф. **Стрельцов А.А.**);
- ✓ **Управления обеспечения безопасного функционирования МГУ** (заместитель проректора — начальник управления, к.ф.н., доц. **Иващенко Г.В.**);
- ✓ **Корпорации Респуббликанский НИИ интеллектуальной собственности** (научный руководитель РНИИС, генеральный директор, заслуженный деятель науки Российской Федерации, д.ю.н., проф. **Лопатин В.Н.**).

Студенты магистратуры проходят научную стажировку и практику: в организациях, учреждениях и на предприятиях высокотехнологичного комплекса России.

Выпускники юридического факультета МГУ всегда востребованы и способны сделать хорошую карьеру в качестве высокопрофессиональных юристов ведущих компаний и экспертов, специализирующихся в информационной сфере инновационной экономики.

Учебный план программы объединяет обязательный (общенаучный) и профессиональный циклы, а также курсы, предлагаемые в рамках вариативной профессиональной части:

## **КУРСЫ**

### **Обязательная часть:**

- ✓ Регулирование информационных отношений в инновационной экономике;
- ✓ Право и экономика инноваций;
- ✓ Интеллектуальная собственность в инновационной экономике;
- ✓ Проблемы обеспечения экономической безопасности инновационной экономики;
- ✓ Конкурентные отношения в инновационной экономике;
- ✓ Преступления в информационной сфере;
- ✓ Информационное общество и информационная безопасность;
- ✓ Правовое обеспечение безопасности использования ИКТ в инновационных процессах (на английском языке);
- ✓ Защита интересов государства в информационной сфере и инновационная экономика;
- ✓ Комплексная защита информации в организациях.

### **Дисциплины по выбору:**

- ✓ Информационное общество и защита персональных данных;
- ✓ Механизм защиты прав на коммерческую тайну;
- ✓ Контроль в сфере обращения информации;
- ✓ Корпоративные системы защиты информации в организациях;
- ✓ Индивидуализация в торговом обороте;
- ✓ Информация о качестве товаров;
- ✓ Правовая работа в организациях высокотехнологичного комплекса;
- ✓ Зарубежный опыт правового регулирования и защиты информации (на английском языке).

Оригинал-макет подготовлен в ООО «Издательство «Юрист»

**Адрес**

Почтовый адрес: 115035, г. Москва, Космодамианская наб., д. 26/55, стр. 7

**Печать**

Отпечатано в типографии «Национальная полиграфическая группа».  
248031, г. Калуга, п. Северный, ул. Светлая, д. 2. Тел. (4842) 70-03-37

Формат 70x100/16. Бумага офсетная. Печать офсетная.

Общий тираж 250 экз.

Номер подписан в печать: сентябрь 2021

ISBN 978-5-8078-0256-9



9 785807 802569