ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ ФИНАНСОВЫХ ОТНОШЕНИЙ В ЦИФРОВОЙ ЭКОНОМИКЕ

Бачурин Д.Г.*

Ключевые слова: *цифровая экономика, правовое регулирование, финансовые отношения, финансовые услуги, цифровое право, информационная безопасность, специализированные принципы, информационная инфраструктура, компьютерные технологии, платежные платформы.*

Аннотация.

Цель: *совершенствование научно-методической базы теории правового регулирования финансовых отношений в условиях цифровой экономики.*

Методы: *системный и сравнительно-правовой анализ природы информационного обеспечения финансово-правовых институтов в условиях цифровой экономики.*

Результаты: *исследованы правовые аспекты формирования инфраструктурной среды цифровой экономики, перевода сервисного обслуживания финансовых операций в полностью автоматизированный режим выполнения, обеспечения информационной безопасности и устойчивости финансовых учреждений в условиях цифровой экономики; обоснована трёхкомпонентная система специализированных принципов правового регулирования финансовых отношений в условиях цифровой экономики; обоснован вывод о необходимости синхронизации развития процессов цифровизации и соответствующего правового регулирования; сформулированы рекомендации по совершенствованию финансово-правового регулирования: определение правовых принципов и процедур цифрового взаимодействия; юридическая регламентация электронного документа и цифрового архива; разработка правовых статусов машин с искусственным интеллектом и лиц, ответственных за функционирование таких объектов (производителей, владельцев, управляющих машинами).*

DOI: 10.21681/1994-1404-2020-1-47-56

Введение

Наибольшие сложности в регулировании финансово-правовых отношений, пронизывающих все сферы социальной деятельности, возникают в моменты качественных изменений в общественной жизни. Среди таких изменений, существенным образом трансформирующих социально-экономические отношения, следует выделить распространение *компьютерных* («*цифровых*») *технологий* [5] в совокупности с расширением доступа к интернету и мобильной связи. Эти изменения служат материальной базой перехода от традиционного индустриального хозяйства к новой информационной экономике, в которой создание и продажа услуг и товаров основаны на принципиально иных методах кодирования, накопления, обработки и передачи информации. По этой причине цифровую экономику можно рассматривать как *системно-структурированную совокупность экономических отношений*, развивающуюся на основе компьютерных технологий. Основное внимание в ней направлено не на совершенствование программного обеспечения, а на товары и услуги, реализуемые посредством электронных продаж.

Привлекательность новых технологий для финансово-кредитных учреждений довольно очевидна. Упрощение операционной интеграции, расширение возможностей интерактивного маркетинга и предложение онлайн-банкинга позволяют объединять предоставляемые услуги в единые пакеты, тем самым увеличивая число клиентов и размер прибыли.

Выгоды владельцев финансовых организаций лежат в плоскости снижения операционных издержек при замене персонала, действующего по заранее установленным правилам, на машинные алгоритмы. Уже сегодня можно наблюдать активное внедрение *новых форм работы*: через создание банковских площадок без сотрудников, где финансовые услуги предоставляются путем цифрового самообслуживания; расширение дистанционных сервисов (онлайн-банкинг) в сети интернет с применением стационарных и мобильных персональных компьютеров [2, 3].

* ***Бачурин Дмитрий Геннадьевич,*** *кандидат юридических наук, ведущий научный сотрудник сектора банковского, финансового, налогового и конкурентного права Института государства и права Российской академии наук, Российская Федерация, г. Москва.*

E-mail: 01ter@mail.ru

1. Правовое регулирование цифрового банкинга

С 2001 г. подавляющее большинство (80%) банков США практикуют электронный банкинг, а *Bank of America* переводит на эти услуги 3 *млн* клиентов (20% его клиентской базы)[1]. В 2009 г. 47% взрослых в США и 30% в Англии имеют активные цифровые (онлайн и мобильные) счета [18]. Согласно опросу, проведенному Японской ассоциацией банкиров (*JBA*) в 2012 г., 65,2% клиентов финансовых учреждений являются пользователями интернет-банкинга[2]. К 2013 г. объем мирового рынка информационных технологий оценивался в 1,7 *трлн долларов США*[3]. На начало 2020 г. услугами цифрового банкинга охвачено примерно 75% клиентов в более чем 95% от общего числа банков США, Англии и стран ЕС.

Важно, что в цифровом формате выполняются все международные расчеты. Они осуществляются через международную межбанковскую систему *SWIFT* (212 стран-участников системы), систему платежей США *Fedwire*, платежную платформу Европейского ЦБ *TARGET* 2 и интегрированные с ними национальные системы платежей отдельных стран.

Предоставление банковских сервисов и услуг практически всегда обслуживается интернет-сетями. По этой причине «цифровой банкинг» еще называют «интернет-банкингом» (*i-banking*). Если провести сравнение традиционной банковской деятельности с цифровым банковским учреждением, то можно выделить следующие характерные черты новых банковских сервисов:

- предоставление банковских услуг с использованием сетей электронных коммуникаций, дополняющих традиционные способы коммуникаций;
- виртуализация самого интернет-банка, материальным воплощением которого становится не банковский офис с мебелью, оргтехникой, денежными хранилищами и сотрудниками, а компьютерный сервер, выполняющий функции сбора, передачи, обработки и хранения информации о клиентах и проводимых ими операциях;
- визуализация цифровых банковских услуг осуществляется не путем живого общения с персоналом банка, а через выполнение клиентом цифрового банка алгоритмической последовательности действий, предлагаемых веб-сайтом такого виртуального банка;
- предоставление не только всего спектра традиционных банковских услуг (услуги по оплате счетов и переводу денежных средств; получение и обслуживание кредитов; ведение инвестиционных проектов; торговля на фондовом рынке; получение сопутствующих финансовых сервисов, дополняющих и обеспечивающих основной перечень банковских услуг), которые выполняются с применением кредитных карт, банкоматов (в том числе и принадлежащих другим организациям)[4], но и предложение разнообразных и постоянно совершенствующихся комплексных «финтех-продуктов», несущих в себе черты и финансов, и технологий (одноранговое кредитование (*P2P*), в том числе с применением кредитных платформ; краудфандинг и дистанционное управление капиталом, в том числе управление личными финансами, онлайн-фондами, электронными кошельками; брокерские онлайн-услуги);
- применение искусственного интеллекта и финансовых технологий, развитие которых идет на основе математических концепций, например, таких, как «облачные вычисления» (*cloud computing*) [4] и «большие данные» (*Big Data*) [14];
- цифровой *i-banking* активно трансформирует рынок финансовых услуг, с явно проявляющейся тенденцией к его децентрализации, со снижением роли традиционных банков и страховых организаций.

В США юридическое регулирование в области цифрового банкинга осуществляется с применением законодательных актов и судебных прецедентов. До начала 2010-х гг. такое регулирование выполняется в основном на основе правовых актов, относящихся к традиционной банковской деятельности.

В ряду ныне действующих актов специализированного законодательства, предусматривающего гарантии защиты прав клиентов финансовых учреждений, выделяется Закон Додда-Франка, принятый в 2009 г. (Dodd-Frank Act), согласно которому учреждается Бюро финансовой защиты потребителей, и Закон об экономическом росте, нормативно-правовом регулировании и защите прав потребителей (Economic Growth, Regulatory Relief, and Consumer Protection Act — EGRRCPA)[5], принятый в 2018 г. Закон EGRRCPA обязывает федеральные банковские агентства всемерно содействовать экономическому росту, делая финансовые услуги более справедливыми для потребителя.

В настоящее время в ряде других стран, в частности, в Китае, Индии, Южной Корее, осуществляются плановые работы по развитию индустрии искусственного интеллекта нового поколения, но практически нет всеобъемлющей правовой базы для защиты данных. Комитет экспертов правительства Индии 27 июля 2018 г. опубликовал проект закона о защите личных данных[6].

---

[1] См.: *Veeraghanta M.* Is Your Digital Banking Vendor Hurting Adoption Rates? The Financial Brand, 2017, URL: https://thefinancialbrand.com/68577/optimal-digital-banking-vendor-selection/ .

[2] URL: http://www.kokusen.go.jp/pdf/n-20001005_3.pdf .

[3] Распоряжение Правительства РФ от 01.11.2013 № 2036-р «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014—2020 годы и на перспективу до 2025 года» // Собрание законодательства РФ. 2013. № 46. Ст. 5954.

[4] См.: *Banerjee R.* Internet Banking — Legal Issues. URL: http://rajdeepandjoyeeta.com/internet-banking-legal-issues/

[5] Economic Growth, Regulatory Relief, and Consumer Protection Act, URL: https://www.congress.gov/bill/115th-congress/senate-bill/2155/text .

[6] Personal Data Protection Bill, 2018, URL: http://meity.gov.in/writereaddata/files/Personal_Data_Protection _Bill,2018.pdf .

Индийский законопроект предусматривает специальную группу прав, связанных с правом протеста против автоматического принятия решений и доступа к логике, стоящей за ним. Эти права связаны с большими данными, поступающими в распоряжение систем искусственного интеллекта, и имеют законное обоснование. Они нацелены на ограничение вреда, возникающего в связи с возможными предубеждениями и дискриминацией в выходных данных из-за оценочных определений без анализа человеком. Решение может состоять в том, чтобы просто включить этап человеческого анализа, который сам по себе не защищен от предрассудков. Такое изменение может потребоваться при условии, что оно тщательно адаптировано к конкретным организациям и характеру их деятельности по обработке данных.

На наш взгляд, этого лучше достичь с помощью системы подотчетности, которая требует определенных фидуциариев данных, которые могут принимать оценочные решения с помощью автоматизированных средств, для организации процессов, которые отсеивают дискриминацию. Этот регулирующий механизм является составным элементом конфиденциальности, который должен быть введен в действие заблаговременно, периодически проверяться и контролироваться.

Представляется, что необходимо предусмотреть возможность юридических ограничений практики некорректной обработки данных. Очевидно, что наиболее действенным способом такой защиты может быть механизм *судебной защиты* нарушенного права [11]. В то же время такая модель не вполне обнажает сущность негативного воздействия. Например, если дискриминация субъекта цифровых отношений возникла в результате, по сути, законной, но дискриминационной по результату автоматической обработки данных.

2. Информационная безопасность и устойчивость финансовых учреждений

В процессе постепенной реорганизации банковской отрасли, связанном с развитием информационных технологий, распространением персональных компьютеров среди домашних хозяйств, интернет-банкингом, телефонным банковским обслуживанием, выявляется необходимость в принятии мер *предосторожности* при использовании новых услуг. С середины 2000-х гг. отмечается, что онлайн-банкинг не может работать вне режима безопасности клиентской информации, напрямую связанного с репутационными рисками самих банков[7].

Атаки на онлайн-банкинг в основном основаны на обмане пользователя с целью кражи данных для входа и действительных *TAN (Transaction authentication number)*. Среди наиболее известных способов кражи регистрационной информации следует выделить:

фишинг (англ. *phishing* — «рыбная ловля») — проведение массовых рассылок электронных писем от имени популярных брендов для получения доступа к конфиденциальным данным пользователей (логинам и паролям);

фарминг (англ. *pharming*) — скрытное перенаправление жертвы на ложный сайт (или *IP*-адрес);

межсайтовый скриптинг (англ. *Cross-Site Scripting*, *XSS*) — внедрение страницы вредоносного кода в компьютер пользователя и взаимодействие этого кода с веб-сервером злоумышленника для получения авторизованных данных пользователя или расширенного доступа. Вредоносный код проникает через уязвимость в веб-сервере или через уязвимость на компьютере пользователя;

кейлоггер (от англ. *keylogger*, *key* — клавиша и *logger* — регистрирующее устройство) — программное обеспечение или аппаратное устройство, отмечающее нажатие клавиш на клавиатуре компьютера и манипуляции с мышью;

троянские вирусные программы — вредоносные программы, внедряемые в компьютер под видом легального программного обеспечения с целью сбора, изменения и удаления информации о пользователе, а также использования ресурсов компьютера для майнинга или нелегальной торговли;

атаки на основе сигнатур, которые состоят в применении программного обеспечения так, чтобы на экране отображались правильные транзакции, а фактически проводимые сфальсифицированные транзакции подписывались в фоновом режиме.

Компьютерные вторжения, осуществляемые на основе перечисленных и вновь разработанных приемов, имеют тенденцию к постоянному увеличению убытков банков и ущерба их клиентов. В 2008 г. в американских банках выявлено 536 случаев компьютерного вторжения во время онлайн-банкинга со средней потерей 30 *тыс. долл.* на один инцидент. В 80% случаев источник вторжения неизвестен [17]. Исследователи Кембриджского университета указывают на удвоение за период с 2011 г. по 2017 г. объемов мошенничества в сфере онлайн-банкинга Англии[8].

Вопросы обеспечения *информационной безопасности* [7, 8, 10] и устойчивости финансовых учреждений в условиях цифровой экономики трудно переоценить. Они должны оперативно решаться по мере расширения информатизации процессов общественной жизни. Особое внимание необходимо уделять «болевым точкам» критично важной инфраструктуры электронного накопления, обработки и обмена информацией.

Среди них следует особо выделить следующие *проблемы*: нарушение финансовой стабильности в деятельности финансово-кредитных учреждений в ре-

[7] См.: Werani T. Business-to-Business-Marketing. Praxisorientiertes Business-to-Business-Marketing. Gabler, 2006, pp. 3-13.

[8] См.: *Kundaliya D.* Online banking fraud has doubled since 2011. Cambridge University, 2019, 31 May, URL: https://www.computing.co.uk/news/3076586/online-banking-frauds-doubled-in-the-seven-year-period-from-2011-to-2017-study-finds .

зультате компьютерных атак на их информационные ресурсы; удержание доверия контрагентов кредитных организаций к надежности предлагаемых электронных сервисов; обеспечение достоверности сведений о фактах нарушений защиты информации при осуществлении банковских операций; снижение непосредственного финансового ущерба клиентов банковских организаций в связи с несанкционированными финансовыми транзакциями (денежные переводы средств без распоряжения клиента).

Формирование инфраструктурной среды *информационной экономики*, развитие цифровых платформ, перевод сервисного обслуживания финансовых операций в полностью автоматизированный режим, применение открытых стандартов и протоколов обусловливает резкое возрастание информационных *рисков* и требует соответствующего развития правового регулирования. По этой причине органы государственной власти сосредотачивают свое внимание на важности решения вопросов регулирования в данной сфере общественных отношений [1].

Начало данного направления в нашей стране было оформлено в 2008 г. с утверждением Стратегии развития информационного общества, которая нацеливает на признание постиндустриальных информационных и телекоммуникационных технологий в качестве ключевых факторов увеличения добавленной стоимости в экономике и общей конкурентоспособности Российской Федерации[9].

Последующее принятие актов правового регулирования[10] в сфере цифровых технологий выделяет основные магистральные направления ее развития: создание современной информационно-телекоммуникационной инфраструктуры и развитие сервисов на основе информационно-телекоммуникационных технологий; обеспечение прав и основных свобод человека в информационном обществе; развитие технологий защиты информации, способных обеспечивать неприкосновенность частной жизни и безопасность информации ограниченного доступа; осуществление юридически значимых действий в электронном формате и др.

В концентрированном виде на решение указанных задач нацелен один из 17 национальных проектов, реализуемых по инициативе Президента Российской Федерации. В частности, национальная программа «Цифровая экономика Российской Федерации» содержит определение ключевых *целей* проекта в виде «создания устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств»[11]. Не случайно авторы программы в качестве двух ее базовых направлений (кроме обеспечения технических и кадровых условий) определяют нормативное регулирование и информационную безопасность.

Следует указать, что вопросы правового регулирования практически полностью охватывают юридическую составляющую регламентации информационной безопасности, выстраиваемой во взаимодействии с развивающимися правовыми институтами идентификации личности, персональных данных, электронной подписи, передачи цифровой информации, различных видов защищаемой законом тайны в системе конфиденциальной информации.

Принимая во внимание комплексный характер современного *информационного права* [6], развитие которого происходит на основе публично-правовых и частноправовых методов регулирования, специалисты ведут речь о необходимости выделения юридических вопросов цифровизации в отдельную подотрасль права [15] с оформлением соответствующих специализированных институтов, а также принятием необходимых норм других отраслей права.

Это предложение нашло законодательное подкрепление в 2019 г., когда в Гражданский кодекс (ГК) РФ были внесены базовые нормы юридического регулирования экономических отношений в цифровой среде[12]. В частности: «цифровые права» отнесены к объектам гражданских прав (ст. 128 ГК РФ); закреплено определение «цифровых прав», дана характеристика и определен субъект правоотношений (ст. 141.1 ГК РФ); идентифицированы дистанционные сделки, осуществляемые с помощью электронных технических средств (ст. 434 ГК РФ); предусмотрены ограничения для использования электронных средств (ст. 1124 ГК РФ); уточнено понятие «самоисполняемой сделки», выполняемой путем применения информационных технологий, определенных условиями такой сделки (ст.309 ГК РФ). Например: смарт-контракты, банковские автоматические платежи.

Важно заметить, что законодатель и регулятор достаточно своевременно среагировали на активное на-

[9] Стратегия развития информационного общества в Российской Федерации (утв. Президентом РФ 7 февраля 2008 г. № Пр-212) // РГ. 2008. № 34. 16 фев.

[10] Постановление Правительства РФ от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество (2011—2020 годы)» // Собрание законодательства РФ. 2014. № 18 (часть II). Ст. 2159; Распоряжение Правительства РФ от 1 ноября 2013 г. № 2036-р «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014—2020 годы и на перспективу до 2025 года» // Собрание законодательства РФ. 2013. № 46. Ст. 5954; Распоряжение Правительства РФ от 8 декабря 2011 г. № 2227-р «Об утверждении Стратегии инновационного развития Российской Федерации на период до 2020 года» // Собрание законодательства РФ. 2012. № 1. Ст. 216; Распоряжение Правительства РФ от 17 ноября 2008 г. № 1662-р «О Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года» // Собрание законодательства РФ. 2008. № 47. Ст. 5489; Указ Президента РФ от 7 мая 2012 г. № 596 «О долгосрочной государственной экономической политике» // РГ. 2012. 9 мая.

[11] URL: http://government.ru/projects/selection/741/35675/ (дата обращения: 10.12.2019).

[12] Федеральный закон от 18 марта 2019 г. № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» // Собрание законодательства РФ. 2019. № 12. Ст. 1224.

растание информационных угроз в финансовой сфере Российской Федерации. В условиях расширения объемов платежных операций за 2017 г. с использованием платежных карт было совершено 317 тыс. несанкционированных операций на сумму 961,3 *млн руб*., а за 2018 г. 417 тыс. таких операций на общую сумму 1384,7 *млн руб*.[13].

При решении задач обеспечения и контроля информационной безопасности (ИБ), противодействия информационным угрозам в кредитно-финансовой сфере основные усилия были направлены на реализацию требований Федерального закона от 27 июня 2018 г. № 167-ФЗ[14] и Федерального закона от 27 июня 2011 г. № 161-ФЗ[15].

С этой целью Банком России были приняты экстренные меры. Введено в действие Указание Банка России № 4926-У1 от 8 октября 2018 г.[16], определяющее специальные процедуры и формы для ведения информационного обмена сообщениями о попытках осуществления переводов денежных средств без согласия клиента. Стандартом СТО БР БФБО-1.5-20182 с 1 ноября 2018 г.[17] уточнены рамки взаимодействия Банка России с субъектами системы информационного обмена в целях выявления инцидентов нарушений защиты информации.

К началу 2019 г. к базе информационного обмена (АСОИ ФинЦЕРТ[18]) подключены все кредитные организации Российской Федерации. С момента начала работы 26 сентября 2018 г. до конца 2018 г. АСОИ ФинЦЕРТ зафиксировано 15 607 финансовых операций без согласия клиента, выполнены мероприятия по приостановлению и блокировке платежей на общую сумму более 40 *млн руб*.

Сформирована первичная правовая база по обеспечению защиты прав человека и гражданина при обработке его биометрических персональных данных при проведении идентификации. В соответствии с частью 14 ст. 14.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ[19] принято совместное Указание Банка России и Публичного акционерного общества «Ростелеком» № 4859-У/01/01/782-184 от 9 июля 2018 г.[20], регламентирующее ответственный сбор, хранение и обработку персональных данных в единой информационной системе.

Вместе с этим законодатель предпринимает меры по повышению эффективности уголовной ответственности за правонарушения в сфере цифровой экономики[21]. В частности, за хищение средств с банковского счета (ч.3 ст.158 УК РФ) и совершение мошенничества с использованием электронных средств платежа (ст. 159.6 УК РФ) предусмотрена ответственность до 6 лет лишения свободы.

3. Система принципов правового регулирования финансовых отношений в цифровой экономике

Сложность правового регулирования в сфере цифровой экономики в целом и финансовых услуг в частности обусловлена достаточно длительными параллельно протекающими процессами:

распространения цифровизации: по горизонтали — через рост числа пользователей, по вертикали — через охват властных и вертикально-интегрированных структур, по глубине — через создание новых электронных сервисов и услуг;

развития юридических конструкций, внедряемых в цифровые отношения;

адаптации основных элементов правовой системы под электронные реалии социально-экономических отношений.

Цифровая экономика через расширенные электронные сети предоставляет инструменты преобразования отраслей услуг и отдельных экономических структур для открытого и подотчетного сотрудничества[22]. О масштабах этого явления свидетельствует тот

---

[13] URL: http://www.cbr.ru/analytics (дата обращения: 10.12.2019).

[14] Федеральный закон от 27 июня 2018 г. № 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств» // Собрание законодательства РФ. 2018. № 27. Ст. 3950.

[15] Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» // Собрание законодательства РФ. 2011. № 27. Ст. 3872.

[16] Указание Банка России от 8 октября 2018 г. № 4926-У «О форме и порядке направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента и получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, а также о порядке реализации операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента».

[17] Стандарт Банка России СТО БР БФБО-1.5-2018 «Безопасность финансовых (банковских) операций. Управление инцидентами информационной безопасности. О формах и сроках взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации», введенный в действие Приказом Банка России от 14 сентября 2018 г. № ОД-2403.

[18] Автоматизированная система обработки инцидентов Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России.

[19] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

[20] Указание Банка России и Публичного акционерного общества «Ростелеком» от 09.07.2018 № 4859-У/01/01/782-18 «О перечне угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в единой информационной системе» // Собрание законодательства РФ, 2006. № 31 (1 ч.), ст. 3448.

[21] Федеральный закон от 23 апреля 2018 г. №111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» // Собрание законодательства РФ. 2018. № 18. Ст. 2581.

[22] URL: http://www.ericsson.com/res/thecompany/docs/publications/business-review/2014/mastering-digital-transformation-a-policy-makers-guide.pdf .

Таблица

Классификация принципов правового регулирования финансовыми отношениями в цифровой экономике

Факторы влияния	Специализированные принципы
Публично-правовой (общесоциальный)	Принцип учета общественных интересов при проектировании правового регулирования цифровых услуг
	Принцип учета мнений всех заинтересованных общественных групп при принятии решений о правовом регулировании отношений в области цифровых услуг
	Принцип координации действий федеральных и региональных органов исполнительной власти, местного самоуправления и гражданского общества по развитию цифровой экономики
Частноправовой	Принцип обеспечения потребителей услуг предсказуемыми уровнями защиты
	Принцип приоритета прав потребителей цифровых услуг
	Принцип цифрового резидентства физических и юридических лиц
Технико-правовой	Принцип тщательности и всесторонности анализа предлагаемых сервисов и услуг
	Принцип неразрывности в обеспечении характеристик эффективности, надежности и безопасности цифрового управления
	Принцип последовательного совершенствования правового регулирования
	Принцип применения преимущественно национального (российского) технического оборудования, программного обеспечения и технологий защиты информации
	Принцип комплексной оценки влияния рисков

факт, что сегодня более 82% потенциальных потребителей в мировой экономике движутся к сетевому образу жизни[23].

Очевидно, что подобное развитие предполагает достаточную гибкость, ясность и широкое распространение соответствующих режимов регулирования, которые объективно должны быть сосредоточены на важнейших социальных задачах и общественно принимаемых правилах их достижения посредством предоставления цифровых услуг и новых возможностей для потребителей[24].

Стратегическим приоритетом здесь выступает разработка *нормативной правовой базы* [11, 12], которая должна отражать базовые ценности, связывающие структуры цифровых услуг, четко определять нормативно-закрепляемые цели и учитывать весь спектр исторических, текущих и вновь возникающих рисков [17].

При проектировании нормативной правовой базы цифровых услуг следует руководствоваться четкими правовыми ориентирами, базирующимися на системе обоснованных принципов [9]. Формализация наиболее важных из них позволяет выделить следующую группу специализированных норм-принципов (см. таблицу), выявленных в ходе системного анализа развития цифровых технологий, искусственного интеллекта, робототехники и отдельных особенностей их юридического положения в ряде зарубежных стран.

Принцип учета и согласования общественных интересов при проектировании правового регулирования цифровых услуг. Данный принцип заключается в том, что никакие правила не должны быть навязаны участникам цифровых правоотношений без свидетельства явно выраженного общественного интереса. Этот принцип особенно важен, когда выясняется, что приоритеты социальной политики или политики безопасности воплощаются в более широком контексте, чем этого требуют коммерческие интересы.

Принцип учета мнений всех заинтересованных общественных групп при принятии решений о правовом регулировании цифровых услуг. Консультации со всеми заинтересованными сторонами важны, чтобы избежать непреднамеренных последствий, возникающих в связи с принятием новой политики или новых правил. Опыт зарубежных стран свидетельствует, что максимально репрезентативные консультации помогают достигать эффективной результативности в определении уровней защиты потребителей при одновременном развитии конкуренции.

Принцип координации действий федеральных и региональных органов исполнительной власти, местного самоуправления и гражданского общества по развитию цифровой экономики. Данный принцип подчеркивает важность тесного взаимосогласованного сотрудничества в решении вопросов развития цифровой экономики всеми заинтересованными участниками отношений. В числе вопросов, разрешаемых на основе применения данного принципа, в частности, могут быть следующие: определение источников бюджетного и внебюджетного финансирования мероприятий (исследований и разработок) технического и норма-

[23] URL: http://www.ericsson.com/res/docs/2015/consumerlab/ericsson-consumerlab-the-network ed-life.pdf .

[24] URL: http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2012/ICC-policy-statement-on-business-views-on-regulatory-aspects-of-cloud-computing/ .

тивно-правового оснащения цифровой экономики; выработка и описание ключевых компетенций действующих в ней субъектов; описание регламентов и стандартов регулирования; организация фундаментальных и прикладных исследований, пилотных проектов и экспертных оценок и др.

Принцип приоритета прав потребителей цифровых услуг предполагает опору на существующее законодательство о защите прав потребителей, положения которого должны иметь очевидное предпочтение перед новыми предписаниями.

Принцип обеспечения потребителей услуг предсказуемыми уровнями защиты. С целью обеспечения защиты потребителей и сохранения стимулов для дальнейшего развития законодатель должен учитывать широкий круг преднамеренных и непреднамеренных последствий применения новых правил. Например, такие угрозы могут быть связаны с построением сложных иерархических информационных и компьютерных систем [16], применяющих виртуализацию, удаленные (облачные) хранилища данных личности, объединений граждан и организаций бизнеса.

Принцип цифрового резидентства физических и юридических лиц. Важность данного принципа обусловлена ранее неизвестными угрозами и вызовами, которые способны к проникновению и активному действию в пространстве цифровой экономики. Не случайно в программе «Цифровая экономика Российской Федерации», утвержденной распоряжением Правительства РФ от 28 июля 2017 г. № 1632-р (*утратило силу*), особо отмечены проблемы обеспечения прав человека в цифровом мире, в том числе при его идентификации, выступающей в виде процедуры соотнесения человека с его цифровым образом или фрагментарными его характеристиками. В данном контексте должны также рассматриваться задачи сохранности цифровых данных пользователей и обеспечения доверия граждан к цифровой среде. Можно также обоснованно предположить, что в уже в ближайшей перспективе возможна постановка вопроса о «резидентстве» машинных систем. Обзоры зарубежной литературы по данной тематике свидетельствуют о том, что он уже перешел из области научной фантастки в число актуальных для исследователей США, Южной Кореи и Японии.

Принцип комплексной оценки влияния рисков. Внедрение такой оценки должно предусматривать максимально полный и четкий анализ всей совокупности возможных рисков принимаемых нововведений.

Принцип тщательности и всесторонности анализа предлагаемых сервисов и услуг. Необходимо определить, какие услуги являются конкурирующими, заменяемыми или аналогичными уже имеющимся на современных финансовых рынках. Особенное внимание следует сосредоточить на выявлении и воспрепятствовании применению так называемых «недопустимых инноваций». Эксперты Международной торговой палаты относят к ним такие технологии и бизнес-модели, которые могут привести к разрушительным последствиям для экономики или нанесению ущерба отдельным потребителей финансовых услуг[25].

Принцип неразрывности в обеспечении характеристик эффективности, надежности и безопасности цифрового управления приобретает особую значимость в контексте неуклонного нарастания враждебного технического воздействия на критично значимую информационную инфраструктуру и стремительное увеличение возможностей международной компьютерной преступности.

Принцип применения преимущественно национального (российского) технического оборудования, программного обеспечения и технологий защиты информации. Совершенно ясно, что без создания собственной элементной базы информационной инфраструктуры не представляется возможным достижение полноценной и устойчивой работы отечественной цифровой экономики. Это вдвойне очевидно, если приходится выстраивать такую сложную систему в достаточно агрессивном окружении [7, 8].

Принцип последовательного совершенствования правового регулирования. Юридические рамки не должны существенно отставать от стремительно развивающихся технологий. Модернизация [12, 13] нормативного обеспечения предполагает систематическое обновление с целью принятия регламентов, которые должны соответствовать новым фактам цифровой экономики, или отказа от правил, которые более не являются обоснованными.

Исследование предлагаемой группы специализированных принципов обнаруживает, что они могут быть классифицированы по отдельным видовым признакам. Например: системно-факторный анализ позволяет выделить три основные взаимосвязанные группы принципов, обусловленные воздействием соответствующих трех основных факторов (см. таблицу): публично-правового (общесоциального), частноправового и технико-правого характера.

Представленная классификация является условной. Фактор *неопределенности*, приобретающий доминирующее влияние в условиях глобальной социально-экономической турбулентности, не позволяет в деталях описать юридические характеристики не только самого здания, но даже несущего каркаса цифровой экономики.

В таких условиях необходимо не только тщательно развивать функцию соответствующего правового регулирования, но и своевременно упорядочивать и систематизировать процессы цифровизации современной экономики.

Достаточно часто эти процессы требуют тщательно выверенной *синхронизации*. В частности, в данной плоскости находится решение вопросов определения *правового статуса*: специализированных роботов и в целом машин с искусственным интеллектом, а также лиц, ответственных за функционирование таких объектов (произ-

[25] ICC policy statement on Regulatory Modernization in the Digital Economy. URL: https://iccwbo.org/publication/icc-policy-statement-on-regulatory-modernization-in-the-digital-economy/ .

водителей, владельцев, управляющих машинами и др.). Этот принципиально важный уже в самой ближайшей перспективе вопрос не может решаться в отрыве от нарождающейся практики применения таких объектов, потому что нельзя заранее предвидеть всех нюансов правового поля складывающейся цифровой реальности.

В деле совершенствования юридического инструментария, применяемого при цифровизации финансовых услуг, представляется необходимым также отметить важность разработки, в частности, таких категорий, институтов и понятий цифрового права, как: правовые процедуры и принципы цифрового взаимодействия, юридическая регламентация электронного документа и цифрового архива.

В этой связи существенным ресурсом проектирования российского цифрового законодательства могут стать сравнительно-правовые исследования современного зарубежного опыта правового регулирования в данной сфере отношений. Многие из вышеназванных вопросов уже находят свое юридическое воплощение в актах законодательства и судебных прецедентах США, Южной Кореи, Японии, Сингапура и других зарубежных стран.

Заключение

Искусственный интеллект и робототехника подрывают системы, которые люди приводили в действие на протяжении тысячелетий, включая производство, гражданские свободы, образование, социальные услуги, научный прогресс и саму природу знаний. Отношения человечества с компьютерами кардинально меняются, но перспективы влияния искусственного интеллекта на общество и экономику остаются неясными.

В этой связи существенным ресурсом проектирования российского цифрового законодательства могут стать дальнейшие исследования современного зарубежного опыта правового регулирования в данной сфере отношений. Многие из вышеназванных вопросов уже находят свое юридическое воплощение в актах законодательства и судебных прецедентах США, Южной Кореи, Новой Зеландии, Китая, Индии, Японии, Сингапура, Индонезии и других зарубежных стран.

Большинство зарубежных стран в 2017—2018 гг. вступили в стадию правового проектирования. Именно в этот период можно наблюдать активное формирование ответственных организационных структур, обсуждения и консультации с экспертным и предпринимательским сообществом, выражение мнений со стороны потребителей, разработку нормативных актов, имеющих преимущественно предварительный характер, как по содержанию, так и времени действия. В таких условиях необходимо не только тщательно развивать функцию соответствующего правового регулирования, но и своевременно упорядочивать и систематизировать процессы цифровизации современной экономики.

Рецензент: ***Запольский Сергей Васильевич,*** *доктор юридических наук, профессор, заслуженный юрист Российской Федерации, главный научный сотрудник Института государства и права Российской академии наук, Российская Федерация, г. Москва.*
E-mail: zpmoscow@mail.ru

Литература

1. Андреев В. К. О понятии цифровых прав и их оборотоспособности // Журнал предпринимательского и корпоративного права. 2018. № 8. С. 38—41.
2. Ващекин А. Н., Ващекина И. В. Противодействие преступной деятельности в условиях развития цифровых технологий дистанционного банковского обслуживания // Правовая информатика. 2019. № 4. С. 86—95. DOI: 10.21681/1994-1404-2019-4-86-95.
3. Ващекин А.Н., Ващекина И. В. Структурная особенность банковской системы РФ и динамика основных показателей ее функционирования // Научное обозрение. Экономические науки. 2019. № 1. С. 5—10.
4. Ефименко А. А., Федосеев С. В. Организация инфраструктуры облачных вычислений на основе SDN сети // Экономика, статистика и информатика. Вестник УМО. 2013. № 5. С. 185—187.
5. Ловцов Д. А. Основы технологии эффективного двухуровневого правового регулирования информационных отношений в инфосфере // Правовая информатика. 2018. № 2. С. 4—14. DOI: 10.21681/1994-1404-2018-2-04-14.
6. Ловцов Д. А. Теория информационного права: базисные аспекты // Государство и право. 2011. № 11. С. 43—51.
7. Ловцов Д. А. Обеспечение информационной безопасности в российских телематических сетях // Информационное право. 2012. № 4. С. 3—7.
8. Ловцов Д. А. Проблема гарантированного обеспечения информационной безопасности крупномасштабных автоматизированных систем // Правовая информатика. 2017. № 3. С. 66—74. DOI: 10.21681/1994-1404-2017-3-66-74.
9. Ловцов Д. А. Система принципов эффективного правового регулирования информационных отношений в инфосфере // Информационное право. 2017. № 1. С. 13—18.
10. Ловцов Д. А., Верхоглядов А. А. Информационная безопасность судебных автоматизированных информационных систем: правовое регулирование и юрисдикция // Российское правосудие. 2008. № 8. С. 55—64.

11. Ловцов Д. А., Ниесов В. А. Обеспечение единства судебной системы России в инфосфере: концептуальные аспекты // Российское правосудие. 2006. № 4. С. 35—40.
12. Ловцов Д. А., Ниесов В. А. Модернизация информационной инфраструктуры судопроизводства — ключевое направление оптимизации нагрузки на судебную систему // Российское правосудие. 2014. № 9. С. 30—40.
13. Ловцов Д. А., Ниесов В. А. Проблемы и принципы системной модернизации «цифрового» судопроизводства // Правовая информатика. 2018. № 2. С. 15—22. DOI: 10.21681/1994-1404-2018-2-15-22.
14. Федосеев С. В. Применение современных технологий больших данных в правовой сфере // Правовая информатика. 2018. № 4. С. 50—58. DOI: 10.21681/1994-1404-2018-4-50-58.
15. Хабриева Т.Я., Черногор Н.Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1. С. 85—102.
16. Черных А. М. Основные направления интеграции федеральных государственных информационных систем и пространственных данных // Правовая информатика. 2018. № 2. С. 47—56. DOI: 10.21681/1994-1404-2018-2-47-56.
17. Deighton-Smith R., Erbacci A., Kauffmann C. Promoting inclusive growth through better regulation: The role of regulatory impact assessment. OECD Regulatory Policy Working Papers. Paris: OECD Publishing, 2016, No. 3, DOI: http://dx.doi.org/10.1787/5jm3tqwqp1vj-en .
18. Rishi P. Maximizing Business Performance and Efficiency Through Intelligent Systems. Hershey, 2017, 255 pp.

INFORMATION SUPPORT FOR LEGAL REGULATION OF FINANCIAL RELATIONS IN DIGITAL ECONOMY

Dmitrii Bachurin, *Ph.D. (Law), Leading Researcher at the Sector of Banking, Financial, Tax, and Competition Law of the Institute of State and Law of the Russian Academy of Sciences, Russian Federation, Moscow.*
E-mail: 01ter@mail.ru

Keywords: *digital economy, legal regulation, financial relations, financial services, digital law, information security, specialised principles, information infrastructure, computer technologies, payment platforms.*

Abstract.
Purpose of the paper: *improving the scientific and methodological basis of the theory of legal regulation of financial relations under the conditions of digital economy.*
Methods used: *a system and comparative law analysis of the nature of information support of financial and legal institutions under the conditions of digital economy.*
Results obtained: *legal aspects of formation of the infrastructure environment of digital economy, transfer of financial transactions servicing to a fully automated execution mode, ensuring information security and stability of financial institutions under the conditions of digital economy are studied. A justification is given for a three-component system of specialised principles of legal regulation of financial relations in digital economy as well as for a conclusion that digitalisation processes development and corresponding legal regulations need to be synchronised. The following recommendations for improving the financial and legal regulation are given: determination of legal principles and procedures for digital interaction; legal regulation of electronic documents and digital archives; development of the legal status of machines with artificial intelligence and persons responsible for the operation of such objects (manufacturers, owners, machine operators).*

References

1. Andreev V. K. O poniatii tsifrovykh prav i ikh oborotosposobnosti. Zhurnal predprinimatel'skogo i korporativnogo prava, 2018, No. 8, pp. 38-41.
2. Vashchekin A. N., Vashchekina I. V. Protivodeistvie prestupnoi deiatel'nosti v usloviiakh razvitiia tsifrovykh tekhnologii distantsionnogo bankovskogo obsluzhivaniia. Pravovaia informatika, 2019, No. 4, pp. 86-95, DOI: 10.21681/1994-1404-2019-4-86-95.
3. Vashchekin A.N., Vashchekina I. V. Strukturnaia osobennost' bankovskoi sistemy RF i dinamika osnovnykh pokazatelei ee funktsionirovaniia. Nauchnoe obozrenie, Ekonomicheskie nauki, 2019, No. 1, pp. 5-10.
4. Efimenko A. A., Fedoseev S. V. Organizatsiia infrastruktury oblachnykh vychislenii na osnove SDN seti. Ekonomika, statistika i informatika, Vestnik UMO, 2013, No. 5, pp. 185-187.
5. Lovtsov D. A. Osnovy tekhnologii effektivnogo dvukhurovnevogo pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere. Pravovaia informatika, 2018, No. 2, pp. 4-14, DOI: 10.21681/1994-1404-2018-2-04-14.

6. Lovtsov D. A. Teoriia informatsionnogo prava: bazisnye aspekty. Gosudarstvo i pravo, 2011, No. 11, pp. 43-51.
7. Lovtsov D. A. Obespechenie informatsionnoi bezopasnosti v rossiiskikh telematicheskikh setiakh. Informatsionnoe pravo, 2012, No. 4, pp. 3-7.
8. Lovtsov D. A. Problema garantirovannogo obespecheniia informatsionnoi bezopasnosti krupnomasshtabnykh avtomatizirovannykh sistem. Pravovaia informatika, 2017, No. 3, pp. 66-74, DOI: 10.21681/1994-1404-2017-3-66-74.
9. Lovtsov D. A. Sistema printsipov effektivnogo pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere. Informatsionnoe pravo, 2017, No. 1, pp. 13-18.
10. Lovtsov D. A., Verkhogliadov A. A. Informatsionnaia bezopasnost' sudebnykh avtomatizirovannykh informatsionnykh sistem: pravovoe regulirovanie i iurisdiktsiia. Rossiiskoe pravosudie, 2008, No. 8, pp. 55-64.
11. Lovtsov D. A., Niesov V. A. Obespechenie edinstva sudebnoi sistemy Rossii v infosfere: kontseptual'nye aspekty. Rossiiskoe pravosudie, 2006, No. 4, pp. 35-40.
12. Lovtsov D. A., Niesov V. A. Modernizatsiia informatsionnoi infrastruktury sudoproizvodstva -- kliuchevoe napravlenie optimizatsii nagruzki na sudebnuiu sistemu. Rossiiskoe pravosudie, 2014, No. 9, pp. 30-40.
13. Lovtsov D. A., Niesov V. A. Problemy i printsipy sistemnoi modernizatsii "tsifrovogo" sudoproizvodstva. Pravovaia informatika, 2018, No. 2, pp. 15-22, DOI: 10.21681/1994-1404-2018-2-15-22.
14. Fedoseev S. V. Primenenie sovremennykh tekhnologii bol'shikh dannykh v pravovoi sfere. Pravovaia informatika, 2018, No. 4, pp. 50-58, DOI: 10.21681/1994-1404-2018-4-50-58.
15. Khabrieva T.la., Chernogor N.N. Pravo v usloviiakh tsifrovoi real'nosti. Zhurnal rossiiskogo prava, 2018, No. 1, pp. 85-102.
16. Chernykh A. M. Osnovnye napravleniia integratsii federal'nykh gosudarstvennykh informatsionnykh sistem i prostranstvennykh dannykh. Pravovaia informatika, 2018, No. 2, pp. 47-56, DOI: 10.21681/1994-1404-2018-2-47-56.
17. Deighton-Smith R., Erbacci A., Kauffmann C. Promoting inclusive growth through better regulation: The role of regulatory impact assessment. OECD Regulatory Policy Working Papers. Paris, OECD Publishing, 2016, No. 3, DOI: http://dx.doi.org/10.1787/5jm3tqwqp1vj-en .
18. Rishi P. Maximizing Business Performance and Efficiency Through Intelligent Systems. Hershey, 2017, 255 pp.