МЕЖДИСЦИПЛИНАРНЫЕ ИССЛЕДОВАНИЯ

УДК 342.9

Охрана интересов несовершеннолетних в условиях цифровой экономики в Российской Федерации и Республике Казахстан

Л. А. Букалерова[1], М. Б. Муратханова[2], А. В. Остроушко[3], М. А. Симонова[1]

[1] Российский университет дружбы народов,
Российская Федерация, 117198, Москва, ул. Миклухо-Маклая, 6
[2] Евразийский национальный университет им. Л. Н. Гумилева,
Республика Казахстан, 010008, Астана, ул. Сатпаева, 2
[3] Финансовый университет при Правительстве РФ,
Российская Федерация, 125993, Москва, Ленинградский пр., 49

Для цитирования: Букалерова, Людмила А., Муратханова, Меруерт Б., Остроушко, Александр В., Симонова, Мария А. 2019. «Охрана интересов несовершеннолетних в условиях цифровой экономики в Российской Федерации и Республике Казахстан». *Вестник Санкт-Петербургского университета. Право* 1: 149–165. https://doi.org/10.21638/spbu14.2019.111

В настоящее время охране информационных прав несовершеннолетних должно быть уделено особенное внимание. Среди основных рисков, сопутствующих построению цифровой экономики в Российской Федерации и Республике Казахстан, выделяют: проблемы потенциальных нарушений при аутентификации личности; низкую сетевую грамотность несовершеннолетних; информационный вакуум, когда отсутствует четкое представления о цифровой экономике; неоднозначную оценку ребенком своих возможностей в среде цифровой экономики; потерю цели в жизни. Авторы статьи отмечают, что поспешный, непродуманный, а главное, не урегулированный правом перевод экономики в цифровую форму может нанести ущерб информационной безопасности несовершеннолетних. В статье анализируется воздействие процессов построения цифровой экономики в Российской Федерации и Республике Казахстан на состояние информационной безопасности несовершеннолетних. Государствам необходимо преодолеть ключевые правовые ограничения и урегулировать вопросы использования инновационных технологий, не допустив при этом появления новых угроз информационной безопасности детей. Указанные проблемы должны стать предметом самого пристального научного анализа с целью создания специальных научно-исследовательских и институциональных структур, в чьи функции будут входить разработка нового

методологического и понятийного аппарата, формирование организационного механизма и выработки правовых, организационных, технических мер, направленных на построение безопасной для личности цифровой экономики. Кроме этого, необходимо осуществлять мониторинг развития всех сегментов цифровой экономики в целях выявления вновь образующихся информационных угроз. По мнению авторов, России и Казахстану необходимо пойти по пути создания законодательства, которое упреждает возникновение проблем и рисков в Интернете для несовершеннолетних, а также позволяет минимизировать их последствия; при этом сделан вывод о том, что ряд положений можно заимствовать из европейского опыта.

Ключевые слова: цифровая экономика, несовершеннолетние, информационная безопасность, риски, правовое регулирование, Россия, Казахстан.

1. Введение. В настоящее время как Российская Федерация, так и Республика Казахстан осуществляют построение цифровой экономики, в рамках которой данные в цифровой форме являются ключевым фактором производства во всех сферах социально-экономической деятельности, а также реально обеспечивается эффективное взаимодействие, в том числе трансграничное, бизнеса, научно-образовательного сообщества, государства и граждан.

В Канкунской декларации Организации экономического сотрудничества и развития (ОЭСР) о цифровой экономике 2016 г.[1], в частности, подчеркнута критическая необходимость дальнейшей разработки на основе консенсуса широкого круга заинтересованных сторон глобальных технических стандартов, способных обеспечить функциональную совместимость и безопасность, стабильность, глобальный, открытый и доступный Интернет. Подписавшие Декларацию государства подтвердили свое стремление сохранить фундаментальную открытость сети Интернет при одновременном обеспечении таких политических целей, как защита конфиденциальности, безопасности, интеллектуальной собственности и детей в Интернете, а также укрепление доверия к Интернету (Ефремов 2016, 36).

В 2016 г. в ежегодном послании Президента РФ В. В. Путина Федеральному Собранию РФ одной из целей было названо построение в России современной модели цифровой экономики к 2024 г. Во исполнение этого поручения принята Стратегия развития информационного общества на период 2017–2030 гг. (далее — Стратегия), в которой дается легальное определение понятия «цифровая экономика» — хозяйственная деятельность, где ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг (Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»[2]). При этом акцент делается не на использовании программного обеспечения, а на

[1] Канкунская декларация о цифровой экономике от 23.06.2016. Дата обращения 12 июля, 2018. https://www.oecd.org/sti/ieconomy/Digital-Economy-Ministerial-Declaration-2016.pdf.

[2] Здесь и далее все ссылки на российские нормативно-правовые акты приводятся по Официальному интернет-порталу правовой информации. Дата обращения 12 июля, 2018. http://www.pravo.gov.ru.

товарах, услугах и сервисах, реализуемых посредством электронного бизнеса, электронной коммерции.

10 января 2018 г. Президент Республики Казахстан Н. А. Назарбаев в Послании народу Казахстана «Новые возможности развития в условиях четвертой промышленной революции» определил, что важным инструментом является проведение цифровизации процессов в государственных органах, которая мультипликативно укрепит гарантии конституционных прав и свобод личности, обеспечит верховенство права и гуманизирует правоохранительную деятельность[3].

Впоследствии в России государственная программа «Цифровая экономика Российской Федерации», утв. Распоряжением Правительства РФ от 28.07.2017 № 1632-р, развила положения названной выше Стратегии, определила дорожную карту построения цифровой экономики, указав, что основной задачей на первом этапе является разработка системы ее правового регулирования (Распоряжение Правительства РФ от 28.07.2017 № 1632-р «Об утверждении программы "Цифровая экономика Российской Федерации"»).

В России цифровая экономика в том виде, как она определена в Стратегии, де-факто развивается уже давно, ее становление происходит довольно быстрыми темпами, поэтому насущной потребностью является продуманное, взвешенное, но ускоренное формулирование комплекса правовых положений. Следует учитывать, что цифровой экономикой потенциально можно охватить все, что поддается формализации, ведь она повлияла на все секторы социальной деятельности и экономики (Чезборо 2007).

2. Основное исследование. Мы вынуждены констатировать, что Россия вступила в цифровую экономику, не имея должного технологического потенциала и собственной сформированной правовой базы. Мировой опыт показывает, что нормативные правовые акты, способствующие современному состоянию цифровой экономики, принимались в ведущих странах мира уже около 10–15 лет тому назад. Кроме того, необходимо урегулировать: вопросы использования технологий по обеспечению информационной безопасности для решения задач предотвращения угроз личности (особенно несовершеннолетним), бизнесу и государству, связанные с тенденциями к построению сложных иерархических информационно-телекоммуникационных систем, а также вопросы защиты от внешнего и внутреннего информационно-технического воздействия на информационную инфраструктуру, в том числе на критическую.

В Европе действует программа «Безопасный Интернет», направленная на урегулирование следующих направлений: обеспечение общественной осведомленности; борьба с незаконным контентом и вредоносным поведением в Интернете; содействие созданию более безопасной онлайн-среды; формирование базы знаний (Решение № 1351/2008/ЕС Европейского парламента и Совета Европейского Союза «О создании многолетней программы Сообщества о защите детей при использовании Интернета и других коммуникационных технологий»[4]).

Республика Казахстан, как и Российская Федерация, взяла курс на цифровизацию экономики. Госпрограмма «Цифровой Казахстан» утверждена Постановлени-

[3] Послание Главы государства народу Казахстана. Официальный сайт Президента Республики Казахстан. Дата обращения 12 июля, 2018. http://www.akorda.kz/ru.

[4] Портал «http://EUR-Lex.europa.eu». Дата обращения 12 июля, 2018. http://eur-lex.europa.eu.

ем Правительства РК от 12.12.2017 № 827[5]. В рейтинге *E-Intensity* международной консалтинговой компании *The Boston Consulting Group* Казахстан является догоняющей страной с точки зрения текущего уровня развития цифровизации, для преодоления чего в программе «Цифровой Казахстан» запланирован ряд инновационных мероприятий.

Анализируя данную программу, мы можем сделать вывод, что проблемы, с которыми столкнулись наши государства, во многом схожи, однако Россия вступила на путь построения цифровой экономики немного раньше и уже достигла некоторых результатов. Учитывая то, что наши правовые системы имеют одну правовую основу, обмен опытом поможет преодолеть существующие трудности.

Цифровизация как в России, так и в Республике Казахстан проходит лавинообразно, при этом негативной тенденцией можно назвать присутствующие в обеих республиках спешку и медийную «накачку» в ходе исполнения стратегических инициатив, что не дает времени оценить необходимость внедрения нового и влечет сопутствующие риски. По мнению Н. Касперской, риски новых технологий сознательно замалчиваются или не обсуждаются, в то же время их достаточно для того, чтобы сначала задуматься о стратегии и необходимости той или иной технологии (Касперская 2018).

Следует отметить своевременность принятия Плана мероприятий по направлению «Информационная безопасность» программы «Цифровая экономика Российской Федерации» (утв. Правительственной комиссией по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 18.12.2017 № 2), согласно которому Минобрнауки России, субъекты РФ ответственны за формирование культуры информационной безопасности у детей и школьников дошкольных образовательных и общеобразовательных организаций. В период до 2020 г. ожидаются, в частности, следующие результаты: состояние материально-технической базы образовательных организаций будет соответствовать требованиям к информационной экономике и новым угрозам в информационной сфере; будет оказана государственная поддержка проектов по профессиональной переподготовке, повышению квалификации и стажировке специалистов по защите информации для задач цифровой экономики; будет разработано 15 программ повышения квалификации педагогических работников; будет оказываться постоянная государственная поддержка проектам по профессиональной переподготовке, повышению квалификации и стажировке педагогических работников; не менее 30 % детей и школьников в возрасте от 6 до 16 лет в каждом субъекте РФ охвачены мероприятиями по формированию культуры информационной безопасности. При этом будут созданы не менее восьми Международных образовательных центров информационной безопасности в субъектах РФ для подготовки специалистов среднего звена, подготовлены более 400 студентов ежегодно; в центрах проходят повышение квалификации более 20 преподавателей ежегодно[6].

[5] Портал правовой информации РК. Дата обращения 12 июля, 2018. https://www.zerde.gov.kz.

[6] План мероприятий по направлению «Информационная безопасность» программы «Цифровая экономика Российской Федерации». Дата обращения 12 июля, 2018. http://static.government.ru/media/files/AEO92iUpNPX7Aaonq34q6BxpAHCY2umQ.pdf.

Некоторые авторы не без основания говорят о цифровой экономике как экономике нового технологического поколения (Кулик, Коряков и Рожанская 2017, 62). Жизнь несовершеннолетних, в частности их социализация, в современном мире напрямую связана с процессом построения цифровой экономики, что требует построения хорошо продуманного комплекса организационных, правовых мер, слаженных действий правоохранительных органов, учителей, провайдеров, родителей, всех членов общества. Однако вопросы влияния цифровой экономики на охрану информационных прав несовершеннолетних, а также их безопасность при переходе к новому инновационному развитию остались без должного внимания исследователей и законодателя.

Авторы настоящей статьи проводят комплексное исследование возможности и допустимости правового противодействия негативному влиянию на психологию подростков посредством информационно-коммуникационной сети Интернет (при поддержке гранта РФФИ № 18-011-00344); сделана попытка проанализировать риски, которые могут быть спровоцированы развитием цифровой экономики в Российской Федерации, в частности предпринята попытка оценить ожидаемость негативного влияния процесса развития цифровой экономики на права и интересы несовершеннолетних. В ходе анкетирования по специальной программе нами опрошено 179 респондентов: в возрастной категории 18–20 лет — 19,7 %, 21–30 лет — 35,5 %, 31–40 лет — 28,9 % и старше 40 лет — 15,9 %; 56,6 % опрошенных — юристы, 9,2 % — педагоги. Мнения респондентов — пользователей современных информационных технологий (61 % из них являются родителями) о возможности или отсутствии негативного влияния цифровой экономики и сопутствующих ей процессов (внедрение блокчейн-технологий, криптовалюты и пр.) на несовершеннолетних распределились примерно одинаково (см. диаграмму 1).

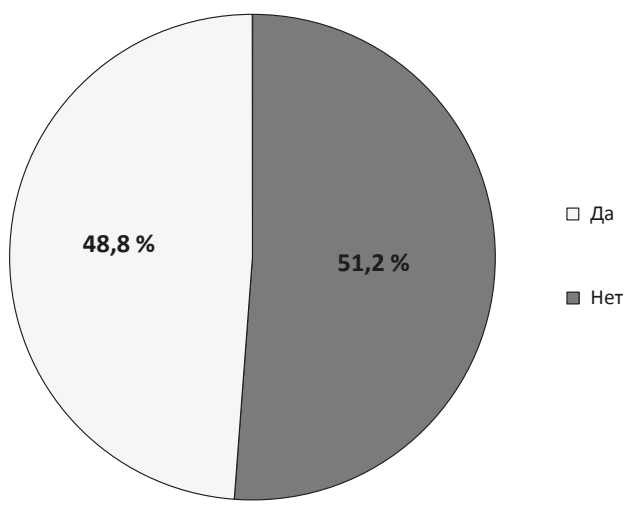

Диаграмма 1. Распределение ответов на вопрос «Возможно ли негативное влияние цифровой экономики на детей?»

С небольшим перевесом преобладает мнение, согласно которому цифровая экономика не приведет к какому-либо воздействию на несовершеннолетних. Мы позволим себе сделать вывод, что общество еще не осознало количественный и качественный состав всех потенциальных рисков перехода к цифровой экономике, и поэтому их влияние на подрастающее поколение в настоящее время недооценено, как в свое время были недооценены компьютер, Интернет и лазер — три современные технологии, наиболее сильно изменившие мир (Taleb 2016, 255). Аналогичные процессы наблюдаются и сегодня, когда появляются новые информационные модели будущего общества, связанные с технологическими прорывами, оказывающими влияние на все стороны жизни (Кутовой 2017, 35).

Государственная программа «Цифровой Казахстан» в п. 3.5 ориентирует общество на достижение такого состояния, когда дети будут мечтать стать предпринимателями и продвигать цифровизацию, и не затрагивает риски, присущие этому процессу. В Республике Казахстан идет постоянная дискуссия о необходимости обезопасить деятельность ребенка в сети Интернет (Как обезопасить своего ребенка… 2017).

Оценив положения нормативных актов РФ и РК, действующих в сфере цифровой экономики, мы выделили следующие основные риски.

1. Нарушения при аутентификации личности. Развитие цифровой экономики первоочередными задачами ставит устранение ключевых правовых ограничений и формирование единой цифровой среды доверия. При этом развитие системы удаленного подтверждения личности для совершения юридически значимых действий сделает доступными пользователям множество функций в различных областях деятельности, которые пользователь сможет совершить одним-двумя кликами мышки. Первый шаг в правовом регулировании этого уже сделан, и согласно изменениям, внесенным в Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», вступившим в силу с 30 июня 2018 г., в Российской Федерации будут использоваться две системы: Единая система идентификации и аутентификации и Единая биометрическая система.

Вторая система безусловно обеспечит гарантированную аутентификацию личности, однако ее использование требует дополнительных финансовых затрат и технических компетенций, поэтому мы прогнозируем, что предпочтение при удаленном взаимодействии будет отдаваться проверенной и знакомой большинству граждан Единой системе идентификации и аутентификации. Однако именно простота использования этой системы позволяет применять ее детям — как по поручению своих родителей, так и самостоятельно, завладев паролем и логином родителей. Таким образом, определить, кто совершает значимое действие на противоположном конце системы телекоммуникации — взрослый или ребенок, становится куда более сложной задачей. По нашему мнению, государство должно направить свои усилия на совершенствование Единой системы идентификации и аутентификации, которая позволит решить проблему подмены личности.

2. Низкая сетевая грамотность несовершеннолетних. Развитие цифровой экономики влечет за собой модернизацию большинства общественных отношений, выражающуюся в их углубляющейся интеграции в сферу информационно-телекоммуникационных технологий, что в итоге проявляется в их цифровом дублировании. Проведенное нами исследование показало, что уже 76,5 % респондентов

в возрасте от 18 до 60 лет считают сеть Интернет особым информационным пространством, в котором происходит их деятельность, 63,4 % опрошенных испытывают ежедневную потребность в сети Интернет и еще 19,5 % не представляют свою жизнь без сети Интернет. Процесс активного взаимодействия детей с телекоммуникационными технологиями, по мнению опрошенных, должен начинаться в соответствии с данными на диаграмме 2.

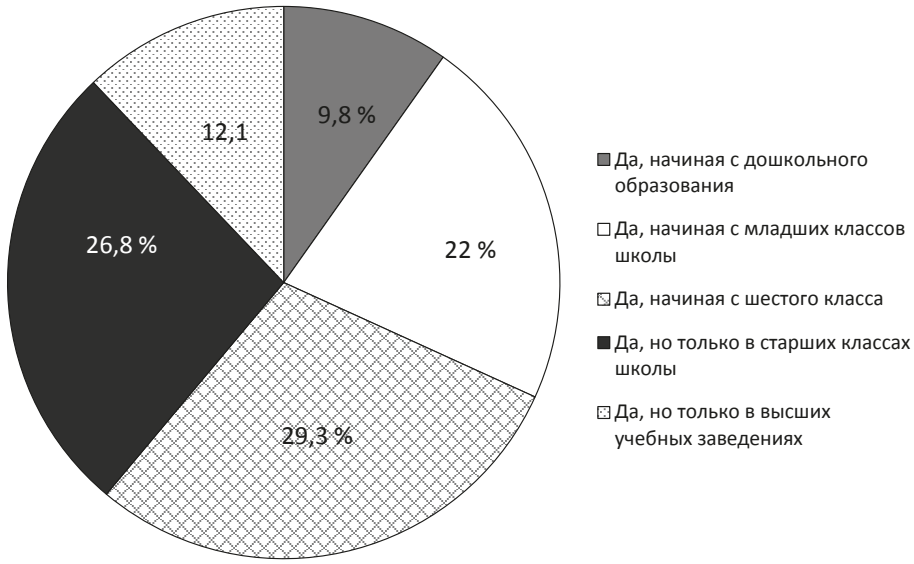

Диаграмма 2. Распределение ответов на вопрос «Должны ли дети активно использовать средства коммуникации и с какого возраста?»

Исследование, проведенное в Республике Казахстан центром «Сандж», показало, что 30,7 % детей (3734 чел.) проводят свободное время сидя в Интернете, социальных сетях чаще, чем играя во дворе (21,7 %), гуляя на улице, выезжая на природу (18,1 %). 16,6 % в свободное время играют в компьютерные онлайн- и офлайн-игры, игры в мобильных приложениях, 15,7 % общаются в программах-мессенджерах, таких как *WhatsApp*, *Viber*, *Skype*[7].

По нашему мнению, ребенок должен быть подготовленным к сетевому взаимодействию в соответствии с возрастными компетенциями, и ключевая роль в этом принадлежит родителям и системе образования. По оценкам зарубежных специалистов, к решению проблемы сетевой безопасности детей должны активно привлекаться педагоги и психологи, в связи с чем требуется уделять внимание разработке теории повседневной деятельности в пространстве сети Интернет всех его участников (Reyns, Henson and Fisher 2011).

Мы не можем с этим не согласиться, однако заметим, что деятельность указанных лиц должна протекать в правовом поле и при поддержке государственных структур, а не на собственном энтузиазме. В ходе обучения ребенка у него долж-

[7] Доклад о положении детей в Республике Казахстан. Астана: Центр исследований «Сандж», 2017.

ны быть сформированы компетенции по безопасному нахождению в виртуальной среде. Считаем, что в настоящий момент для этого делается очень мало. Так, Министерство образования и науки РФ по инициативе Совета Федерации рекомендовало проведение в школах России всероссийского урока безопасности школьников в сети Интернет, и такой урок проводится в учебных заведениях лишь один раз в год.

Приказ Минобрнауки России от 17.12.2010 № 1897 «Об утверждении федерального государственного образовательного стандарта основного общего образования» содержит требования по формированию коммуникативной компетентности в общении и сотрудничестве со сверстниками, детьми старшего и младшего возраста, взрослыми в процессе образовательной, общественно полезной, учебно-исследовательской, творческой и других видов деятельности, однако данный Стандарт не подразумевает формирование у несовершеннолетних медийной грамотности и навыков безопасного поведения в информационной среде. Приоритетный национальный проект «Современная цифровая образовательная среда в Российской Федерации» не уделяет внимания вопросам информационной безопасности детей.

Родителям следует опираться на советы ведущих компаний в сфере информационных технологий и провайдеров: снабдить мобильные устройства с выходом в Интернет и компьютеры системами защиты и родительского контроля; регулярно и полно информировать ребенка о возможных опасностях Интернета и приучить советоваться с взрослыми каждый раз перед тем, как воспользоваться теми или иными предложениями и/или услугами в Интернете; познакомить ребенка с необходимыми мерами безопасности перед тем, как совершить покупку в интернет-магазине; договориться с детьми о том, чтобы использовать только лицензионное программное обеспечение и данные, полученные из надежных источников; разъяснить детям, почему так важно периодически менять пароли, избегать встреч с незнакомцами; необходимо контролировать контакты ребенка.

При этом родители должны: знать интересы и цели, с которыми дети пользуются Интернетом; допускать использование детьми Интернета только в присутствии и под контролем взрослых; исключить доступ детей к ресурсам Интернета, содержание которых противоречит законодательству РФ, может оказать негативное влияние на несовершеннолетних, — в том числе путем обращения в соответствующие органы и инстанции; контролировать использование информации несовершеннолетними.

Анализ инициатив, заложенных в Государственной программе «Цифровой Казахстан», показывает, что основные направления совершенствования во всех сферах образования, в частности при актуализации типовых учебных планов и программ, направлены на освоение компетенций в сфере использования информационно-коммуникационных технологий, не предполагая (как и в России) формирования у обучающихся компетенций в области безопасного поведения в информационном пространстве.

3. Информационный вакуум, возникающий тогда, когда граждане, тем более несовершеннолетние, не имеют четкого представления о том, что такое цифровая экономика, о допустимости и законности применения в тех или иных технологий в конкретных случаях. Доктрина информационной безопасности Российской Федерации одним из основных направлений обеспечения таковой называет обеспече-

ние защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности. Считаем информационное обеспечение процесса внедрения инноваций в нашей стране недостаточным. Государству стоит в обязательном порядке включать в документы стратегического планирования мероприятия, позволяющие акцентировать внимание на сущности предлагаемых инноваций. Анализ программы «Цифровая экономика Российской Федерации» показал, что вопросы информационной поддержки в ней отсутствуют, акцент делается только на кадровом обеспечении реализации данной программы.

4. Риск неоднозначной оценки ребенком возможностей, предоставляемых цифровой экономикой, и в дальнейшем — неправильной интерпретации, влекущей негативные последствия. В качестве примера приведем популярное в 2017 г. среди несовершеннолетних направление деятельности по добыче криптовалюты. Данная деятельность широко разрекламирована, в том числе средствами массовой информации. Однако о том, что эта деятельность сверхдоходна только тогда, когда ею занимаются в промышленных масштабах, а на бытовом уровне она очень рискованна, пресса умалчивает. Подросток, не имея информации, вовлекается в данную деятельность, затрачивает определенные средства на модернизацию компьютеров, расходует энергетические ресурсы с целью «майнить» биткоины, но в итоге расходы на получение криптовалюты превышают полученный доход. При этом оценить все недостатки от такой деятельности можно еще на начальном этапе, если бы в подростковой среде проводились профилактика и соответствующая разъяснительная работа.

5. Риск потери цели в жизни связан с распространением идеи дальнейшего ускоренного замещения человека информационными продуктами. Так, Г. Греф (Греф 2017) и первый заместитель министра финансов России Т. Нестеренко (Стенограмма Первого Московского… 2016) признали, что вскоре при внедрении цифровой экономики станут ненужными для общества профессии юристов, бухгалтеров и учителей. Также возникает проблема законодательного наделения роботов правами и обязанностями субъектов различных правоотношений. В начале 2017 г. в Бельгии робот по имени Фрэн Пеппер стал первым в мире гуманоидом, которого официально включили в реестр населения, а человекоподобный робот София получил гражданство в Саудовской Аравии (Barsanti 2017). Подчеркивается, что цифровая экономика означает одновременно и новые возможности, и новые вызовы для общества, когда уровень образования станет решающим фактором при поиске и сохранении работы. В связи с этим необходимо создать методологическую основу для развития компетенций в области регулирования цифровой экономики, т. е. принять соответствующие методические документы (Вайпан 2017, 10).

Очевидно, что цифровая экономика — перспективный элемент социально-экономического развития нашей страны. Считаем, что инициативы по переходу к цифровой экономике сопряжены с определенными рисками и требуют пристального внимания законодателя для обеспечения информационной безопасности всех граждан, особенно несовершеннолетних. В сложившейся ситуации поспешный перевод экономики в цифровую форму может нанести ущерб информационной безопасности несовершеннолетних.

Говоря об обеспечении информационной безопасности в ходе построения цифровой экономики личности, особенно несовершеннолетнего, мы приходим к выво-

ду о том, что и Российской Федерации, и Республике Казахстан необходимо пойти по пути создания опережающего законодательства, упреждающего возникновение проблем и рисков, а также позволяющего минимизировать их последствия. Игнорирование данного требования повлечет за собой повторение парадоксальной ситуации, когда законодатель осознал риски и опасности сети Интернет на 10–15 лет позже, чем сеть стала неотъемлемым элементом жизни людей.

В рамках работы над комплексной темой, направленной на противодействие техногенным, социокультурным угрозам, терроризму и идеологическому экстремизму, а также киберугрозам и иным источникам опасности для общества, экономики и государства, мы выдвигаем гипотезу о необходимости более своевременного и качественного конструирования правовых норм, направленных на охрану информационной безопасности несовершеннолетних, и корреляции мер правового воздействия с мерами о родительского и школьного контроля.

Проанализируем направления развития законодательства для обеспечения безопасности несовершеннолетних в ходе построения цифровой экономики. Основной проблемой, которая вызывает много споров в обществе, является допустимость вмешательства государства в регулирование информационных отношений, особенно отношений с использованием сети Интернет. Как правило, общество негативно реагирует на любые инициативы власти в данной сфере. Даже противодействие распространению суицидальной информации среди несовершеннолетних некоторые авторы интерпретировали как ужесточение контроля над распространением информации в сети Интернет (Архипова и др. 2017). В последние годы зафиксировано немалое количество случаев, когда дети, не выдержав психологического натиска от информации, связанной с предстоящими ЕГЭ и порождающей страх неудачи, порицания со стороны учителей и родителей, неизбежности наступления нежелательных последствий, влияющих на будущую судьбу подростка (например, непоступление в вуз, призыв в армию, возможное аннулирование результатов и пр.), расстались с жизнью[8].

Допустимость правового воздействия на информационные отношения путем расширения полномочия государственных органов с целью защиты несовершеннолетних от рисков и вредоносного воздействия в информационно-телекоммуникационных сетях была предметом опроса в ходе нашего исследования. Данная инициатива была поддержана 38,2 % респондентов, еще 40,8 % пришли к выводу, что необходимо найти баланс в сочетании государственного воздействия и общественного контроля с целью не допустить узурпацией властью информационного пространства (диаграмма 3). Мы также полагаем, что сегодня вмешательство государства в информационные отношения является необходимостью, однако в демократическом обществе должен быть создан механизм, при котором достижим баланс между правом человека на информацию и свободное информационно-коммуникативное взаимодействие — и ограничениями, вытекающими из необходимости обеспечения информационной безопасности. По нашему мнению, эта роль отводится общественной экспертизе всех вновь принимаемых нормативных правовых актов в данной сфере и общественному контролю за их реализацией.

[8] Самоубийства школьников в РФ из-за экзаменов в 2005–2010 гг. Справка. Дата обращения 12 июля, 2018. http://ria.ru/spravka/20100602/241538298.html.

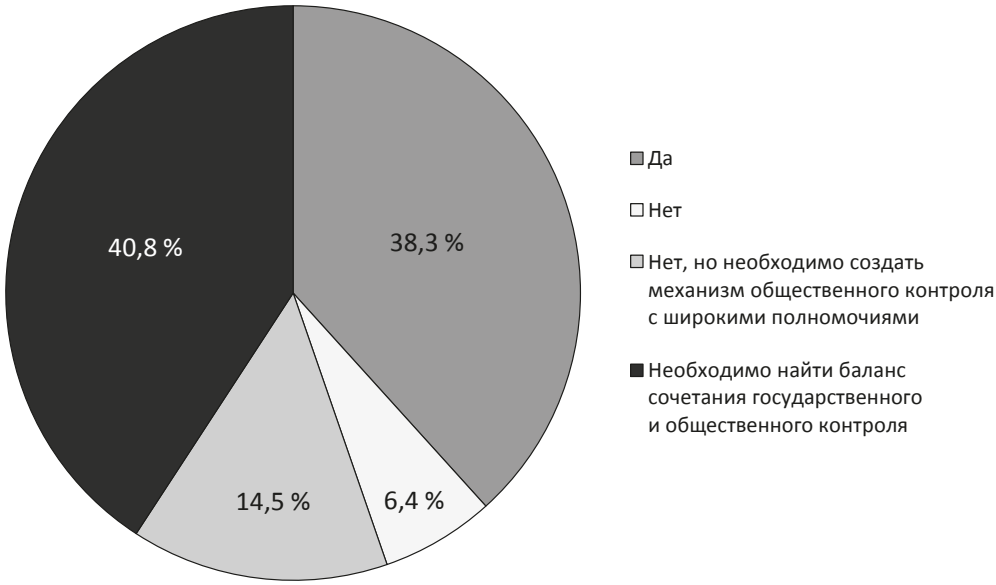

Диаграмма 3. Распределение ответов на вопрос «Необходимо ли государственное регулирование сети Интернет?»

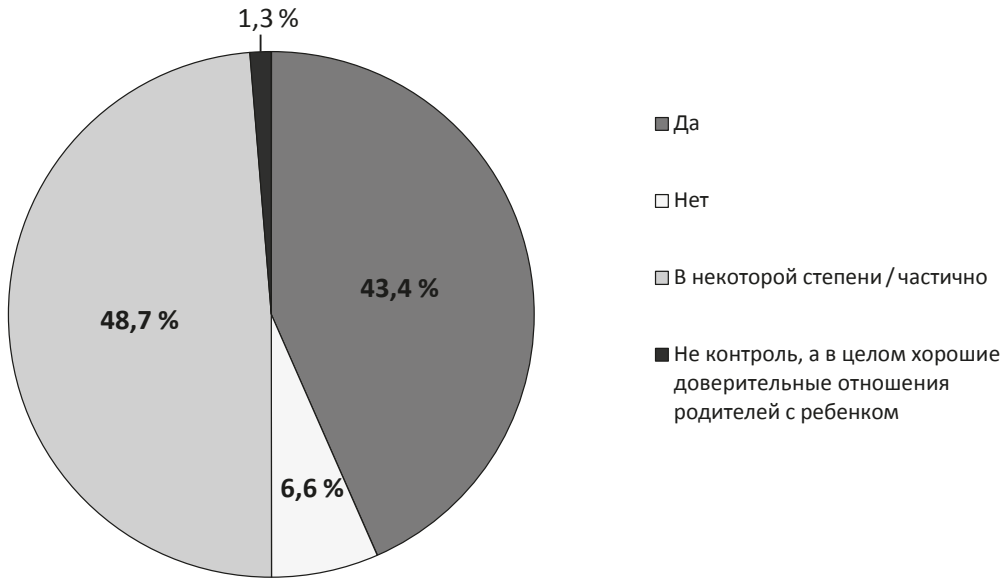

Диаграмма 4. Распределение ответов на вопрос «Возможно ли противодействие информационному воздействию на детей посредством сети Интернет путем осуществления родительского контроля?»

Проведенный нами социологический опрос показал (диаграмма 4): подавляющее большинство респондентов считают, что бороться с негативным информационным воздействием необходимо исключительно путем дополнения Уголовного кодекса РФ новыми составами преступлений. Нормы других отраслей — административного, информационного, гражданского — в противодействии данному явлению остались недооцененными ими. Указанные обстоятельства повышают риски негативных последствий на начальной стадии негативного информационного воздействия. Таким образом, можно сделать вывод, что в общественном мнении приоритет отдается запретам и наказанию, а не материальному регулированию отношений.

В Российской Федерации прослеживается определенный дисбаланс между мерами карательного характера и общественного воздействия, инструментами которого, по нашему мнению, должны выступать общественные институции, в частности семья и школа. Исследование показывает, что респондентами недооценены возможности контроля со стороны родителей, школы и общественности в противодействии данным негативным явлениям (диаграмма 5).

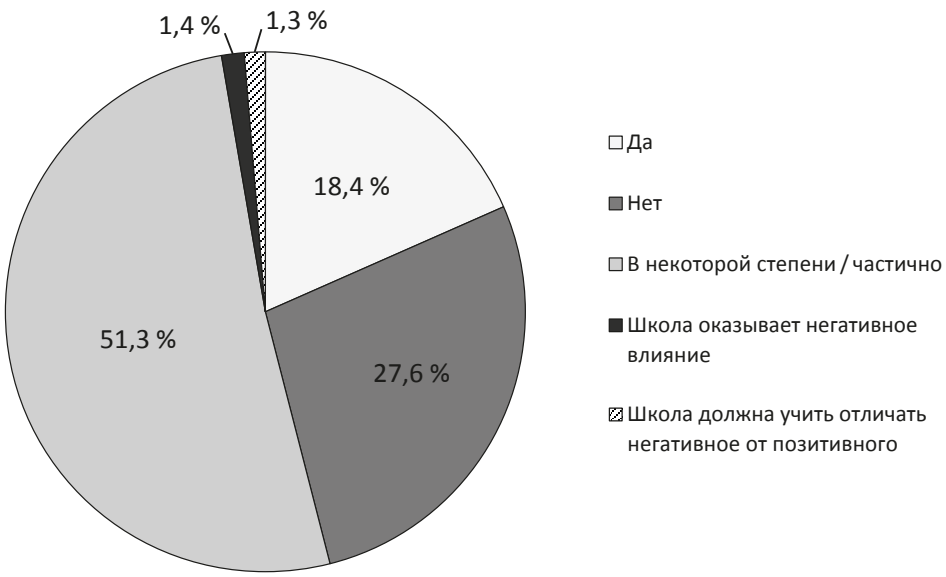

Диаграмма 5. Распределение ответов на вопрос «Возможно ли противодействие информационному воздействию на детей посредством сети Интернет в ходе деятельности педагогов и общественности?»

В то же время исследование, проведенное в Республике Казахстан в рамках спецпроекта «Безопасность детей в Интернете»[9], показывает, что родители осведомлены об опасностях в сети Интернет и понимают, что ребенка можно защитить простыми технологическими средствами, при этом не контролируя его слишком явно. Министерство внутренних дел Республики Казахстан постоянно рекомендует родителям «усилить контроль за виртуальной жизнью своих детей». Однако при

[9] Портал www.dixinews.kz. Дата обращения 12 июля, 2018. https://www.dixinews.kz/spetsproekt.

большей вовлеченности такого общественного института, как семья, в процесс обеспечения информационной безопасности несовершеннолетних в Республике Казахстан осуществляется защита от «классических» информационных рисков; каких-либо упоминаний о таких возможных рисках для несовершеннолетних, которые порождаются переходом к цифровой экономике, в казахстанском медиапространстве нам обнаружить не удалось.

В целом государства, обеспокоенные проблемой эффективной защиты несовершеннолетних от вредного информационного влияния, источником которого стала сеть Интернет, пришли к закреплению двух моделей: 1) фильтрация контента; 2) медиаобразование (Иванов 2012).

Считаем возможным взять за основу Программу, разработанную десять лет назад Европейским парламентом и Советом Европейского союза (Решение № 1351/2008/ЕС «О создании многолетней программы Сообщества о защите детей при использовании Интернета и других коммуникационных технологий»[10]). Она реализуется по четырем направлениям: обеспечение общественной осведомленности; борьба с незаконным контентом и вредоносным поведением в Интернете; содействие созданию более безопасной онлайн-среды; формирование базы знаний.

Основными мероприятиями по первому направлению «Обеспечение общественной осведомленности» являются: повышение общественной информированности и распространение информации о более безопасном использовании онлайн-технологий; обеспечение работы контактных пунктов, где родители и дети могут получать ответы на вопросы о том, как оставаться в безопасности в Интернете, и советы о том, как действовать в случаях склонения к совершению развратных действий и кибериздевательств; поощрение увеличения эффективности и рентабельности методов и инструментов повышения осведомленности; обеспечение обмена передовым опытом и трансграничного сотрудничества на уровне ЕС; обеспечение обмена лучшими практиками и сотрудничество на международном уровне.

По второму направлению «Борьба с незаконным контентом и вредоносными действиями в Интернете» намечены: обеспечение общественности контактными пунктами и горячими линиями для сообщения о незаконном контенте в Интернете и о вредоносном поведении, а также обеспечение их деятельности; борьба против вредоносного поведения в Интернете, в частности против развратных действий и кибериздевательств; стимулирование применения технических решений для надлежащих действий против незаконного контента и вредоносного поведения онлайн, а также для информирования конечных пользователей о том, каким образом данная технология может быть применена; содействие сотрудничеству и обмену информацией, опытом и лучшими практиками между заинтересованными сторонами на национальном и европейском уровнях; расширение сотрудничества, обмен информацией и опытом в сфере борьбы с незаконным контентом и вредоносным поведением на международном уровне; вовлечение реестров доменных имен запрещенных ресурсов различных государств во взаимный обмен информацией, если он еще не осуществляется, и укрепление существующего сотрудничества.

По третьему направлению, «Содействие созданию более безопасной онлайн-среды», запланировано следующее: укрепление сотрудничества, обмен информа-

[10] Official Journal of the European Union. N L 348. 24.12.2008. P. 118.

цией, опытом и лучшими практиками между заинтересованными сторонами; поощрение заинтересованных сторон к разработке и внедрению адекватных систем саморегулирования и совместного регулирования; поддержка провайдеров в разработке знаков маркировки и оказание им помощи в этом; стимулирование вовлечения детей в создание более безопасной онлайн-среды; увеличение объема информации о надлежащих инструментах борьбы с вредоносным контентом в Интернете; обеспечение совместимости между подходом, принятым в Европейском союзе, и подходом, принятым на международном уровне.

По четвертому направлению «Формирование базы знаний» планируется: поощрение скоординированного подхода к исследованиям в соответствующих областях; предоставление обновленной информации об использовании детьми онлайн-технологий; анализ статистики и тенденций в разных государствах — членах ЕС; содействие расследованию онлайн-виктимизации детей; содействие изучению эффективных способов улучшения безопасного использования онлайн-технологий; расширение знаний о последствиях воздействия современных и новых технологий на детей.

3. Выводы. Безусловно, использование сети Интернет и других коммуникационных технологий, таких как мобильные телефоны, значительно расширяется в России и Казахстане, предлагая гражданам бóльшие возможности. Вместе с тем продолжают существовать риски злоупотребления данными технологиями со стороны детей. В целях защиты физической, психологической и моральной неприкосновенности детей, которой может быть нанесен вред в результате доступа к неуместному контенту, должны быть приняты меры на государственном уровне. Более того, для побуждения использования гражданами возможностей и преимуществ, предоставляемых Интернетом и другими коммуникационными технологиями, необходимы также меры, способствующие большей безопасности в этой сфере.

Все перечисленные проблемы должны стать предметом пристального научного анализа с целью создания специальных научно-исследовательских и институциональных структур, в чьи функции будут входить разработка нового методологического и понятийного аппарата, формирование организационного механизма и выработка правовых, организационных, технических мер по осуществлению практического мониторинга состояния цифровой экономики и всех ее сегментов.

Библиография

Архипова, Александра С., Волкова, Мария Д., Кирзюк, Анна А., Малая, Елена К., Радченко, Дарья А., Югай, Елена Ф. 2017. «*Группы смерти»: от игры к моральной панике*. М.: РАНХиГС, ШАГИ.

Вайпан, Виктор А. 2017. «Основы правового регулирования цифровой экономики». *Право и экономика* 11: 5–18.

Греф, Герман О. 2017. «Новые технологические тренды и модели эффективного менеджмента». Дата обращения 12 июля, 2018. http://yeltsin.ru/affair/german-gref-novye-tehnologicheskie-trendy-i-modeli-effektivnogo-menedzhmenta.

Ефремов, Алексей А. 2016. «Единые цифровые пространства: в поиске баланса между интеграцией и суверенностью». *Информационное право* 3: 36–39.

Иванов, Иван С. 2012. *Правовая защита детей от информации, причиняющей вред их здоровью и развитию: Расширенный научно-практический комментарий*. Подготовлен для СПС «Консультант Плюс». Дата обращения 1 сентября, 2018. http://www.consultant.ru.

Как обезопасить своего ребенка в Интернете? Советы казахстанских специалистов 2017. *ИА Тотал Казахстан*. 12 апр.

Касперская, Наталья И. 2018. «Цифровая экономика и риски цифровой колонизации. Развернутые тезисы выступления на Парламентских слушаниях в Госдуме». Дата обращения 12 июля, 2018. https://ivan4.ru/~ZPDWy.

Кулик, Анна М., Коряков, Даниил П., Рожанская, Анастасия Г. 2017. «Цифровая экономика как экономика нового технологического поколения». *Научно-технический прогресс как фактор развития современной цивилизации: сборник статей по итогам Международной научно-практической конференции.* Уфа: Агентство международных исследований.

Кутовой, Данила А. 2017. «Цифровая аналогия общественных отношений в постиндустриальном обществе: потенциал развития или новая угроза?». *Информационное право* 4: 34–38.

Стенограмма Первого Московского финансового форума. 2016. Дата обращения 12 июля, 2018. http://www.mff.minfin.ru.

Чезборо, Генри В. 2007. *Открытые инновации. Создание прибыльных технологий.* М.: Поколение.

Barsanti, Sam. 2017. «Saudi Arabia takes terrifying step to the future by granting a robot citizenship», *The A. V. Club*. Accessed July 12, 2018. https://www.avclub.com/saudi-arabia-takes-terrifying-step-to-the-future-by-gra-1819888111.

Reyns, Bradford W., Henson, Billy, Fisher, Bonnie S. 2011. «Being Pursued Online Applying Cyberlifestyle — Routine Activities Theory to Cyberstalking Victimization». *Criminal Justice and Behavior* 38 (11): 1149–1169.

Taleb, Nassim N. 2016. *The Black Swan: The Impact of the Highly Improbable*. Random House Trade Paperbacks.

Статья поступила в редакцию 27 июня 2018 г.,
рекомендована в печать 15 ноября 2018 г.

Контактная информация:

Букалерова Людмила Александровна — д-р юрид. наук, проф.; bukalerova_la@pfur.ru
Муратханова Меруерт Бейсеновна — канд. юрид. наук, доц.; m.muratkhanova@yandex.ru
Остроушко Александр Владимирович — канд. юрид. наук, доц.; avostroushko@fa.ru
Симонова Мария Александровна — д-р ист. наук, проф.; simona23@bk.ru

Protection of interests of minors in the digital economy in the Russian Federation and the Republic of Kazakhstan

L. A. Bukalerova[1], M. B. Muratkhanova[2], A. V. Ostroushko[3], M. A. Simonova[1]

[1] RUDN University,
6, Miklouho-Maclay st., Moscow, 117198, Russian Federation
[2] Eurasian National University named after L. N. Gumilyov,
2, Satpayev st., Astana, 010008, Republic of Kazakhstan
[3] Financial University under the Government of the Russian Federation,
49, Leningradsky av., Moscow, 125993, Russian Federation

For citation: Bukalerova, Liudmila A., Muratkhanova, Meruert B., Ostroushko, Alexander V., Simonova, Maria A. 2019. "Protection of interests of minors in the digital economy in the Russian Federation and the Republic of Kazakhstan". *Vestnik of Saint Petersburg University. Law* 1: 149–165. https://doi.org/10.21638/spbu14.2019.111 (In Russian)

The article analyzes the impact of processes of building the digital economy in the Russian Federation and Republic of Kazakhstan on the state of the information security of minors. Our states are encouraged to jointly urgently overcome the basic legal restrictions of the

digital economy and regulate the use of innovative technologies. It is necessary to prevent the emergence of new threats to the information security of the individual. Special attention should be paid to the protection of information rights of minors. Among the main risks associated with the construction of digital economy in our republics are: the problems of potential violations in the authentication of the individual, low Internet literacy of minors, information vacuum — when there is no clear idea of the digital economy, ambiguous assessment of the child's capabilities in the digital economy, loss of purpose in life. The authors note that the transfer of the economy into digital form which is hasty, ill-conceived, and, most importantly, not regulated by law can harm the information security of minors. These problems should be the subject of the most rigorous scientific analysis in order to create special research and institutional structures. These structures should ensure the development of a new methodological and conceptual framework; the formation of an institutional mechanism: the development of legal, organizational, technical measures aimed at building a digital economy safe for the individual. In addition, it is necessary to monitor the development of all segments of the digital economy in order to identify emerging information threats.According to the authors, Russia and Kazakhstan need to follow the path of creating legislation that prevents the occurrence of problems and risks and which can also minimize their consequences. A number of provisions can be borrowed from the European experience.

Keywords: digital economy, minors, information security, risks, legal regulation, Russia, Kazakhstan.

References

Arkhipova, Alexandra S., Volkova, Mariya D., Kirziuk, Anna A., Malaya, Elena K., Radchenko, Dariya A., Yugai, Elena F. 2017. *«Gruppy smerti»: ot igry k moral'noi panike* [*"Groups of Death": from play to moral panic*]. Moscow: RANHiGS, SHAGI Publ. (In Russian)

Barsanti, Sam. 2017. "Saudi Arabia takes terrifying step to the future by granting a robot citizenship". *The A. V. Club*. Accessed July 12, 2018. https://www.avclub.com/saudi-arabia-takes-terrifying-step-to-the-future-by-gra-1819888111.

Chasborough Henry W. 2007. *Otkrytye innovatsii. Sozdanie pribyl'nykh tekhnologii* [*Open innovation. Creating profitable technologies*]. Moscow: Pokolenie Publ. (In Russian)

Efremov, Alexey A. 2016. «Edinye tsifrovye prostranstva: v poiske balansa mezhdu integratsiei i suverennost'iu» ["Single digital spaces: in the search for a balance between integration and sovereignty"]. *Information law* 3: 36–39. (In Russian)

Gref, German O. «*Novyje tekhnologicheskije trendy i modeli effektivnogo menedzhmenta*» ["*New technological trends and models of effective management*"]. Accessed July 12, 2018. http://yeltsin.ru/affair/german-gref-novye-tehnologicheskie-trendy-i-modeli-effektivnogo-menedzhmenta (In Russian)

Ivanov, Ivan S. *Pravovaia zashchita detei ot informatsii, prichiniaiushchei vred ikh zdorov'iu i razvitiiu: Rasshirennyi nauchno-prakticheskii kommentarii* [*Legal protection of children from information that is harmful to their health and development: An expanded scientific and practical commentary*]. Prepared for the "ConsultantPlus" system. Accessed September 1, 2018. http://www.consultant.ru (In Russian)

Kak obezopasit' svoego rebenka v Internete? Sovety kazakhstanskikh spetsialistov [How to protect your child on the Internet? Councils of Kazakhstani specialists]. 2017. *IA Total Kazakhstan*. 12 Apr. (In Russian)

Kasperskaya, Natalia I. 2018. *«Tsifrovaia ekonomika i riski tsifrovoi kolonizatsii. Razvernutye tezisy vystupleniia na Parlamentskikh slushaniiakh v Gosdume»* ["*Digital economy and risks of digital colonization. The detailed theses of the speech at the Parliamentary hearings in the State Duma*"]. Accessed July 12, 2018. https://ivan4.ru/~ZPDWy. (In Russian)

Kulik, Anna M., Koryakov, Daniil P., Rozhanskaya, Anastasiya G. 2017. «Tsifrovaia ekonomika kak ekonomika novogo tekhnologicheskogo pokoleniia» ["Digital economy as an economy of a new technological generation"]. *Nauchno-tekhnicheskii progress kak faktor razvitiia sovremennoi tsivilizatsii: sbornik statei po itogam Mezhdunarodnoi nauchno-prakticheskoi konferentsii* [*Scientific and technical progress as a*

factor in the development of modern civilization: a collection of articles on the results of the International Scientific and Practical Conference]. Ufa: Agency for International Studies Publ. (In Russian)

Kutovoy, Danila A. 2017. «*Tsifrovaia analogiia obshchestvennykh otnoshenii v postindustrial'nom obshchestve: potentsial razvitiia ili novaia ugroza?*» ["Digital analogy of social relations in a post-industrial society: development potential or a new threat?"]. *Information law* 4: 34–38. (In Russian)

Reyns, Bradford W., Henson Billy, Fisher, Bonnie S. 2011. "Being Pursued Online Applying Cyberlifestyle — Routine Activities Theory to Cyberstalking Victimization". *Criminal Justice and Behavior* 38 (11): 1149–1169.

Stenogramma Pervogo Moskovskogo finansovogo foruma [*Transcript of the First Moscow Financial Forum*]. 2016. Accessed on July 12, 2013. http://www.mff.minfin.ru. (In Russian)

Taleb, Nassim N. 2016. *The Black Swan: The Impact of the Highly Improbable*. Random House Trade Paperbacks.

Vaipan, Victor A. 2017. "Osnovy pravovogo regulirovaniia tsifrovoi ekonomiki" ["Fundamentals of Legal Regulation of the Digital Economy"]. *Law and Economics* 11: 5–18. (In Russian)

Received: June 27, 2018
Accepted: November 15, 2018

Author's information:

Liudmila A. Bukalerova — Dr. Sci. in Law, Professor; bukalerova_la@pfur.ru
Meruert B. Muratkhanova — PhD, Associate Professor; m.muratkhanova@yandex.ru
Alexander V. Ostroushko — PhD, Associate Professor; avostroushko@fa.ru
Maria A. Simonova — Dr. Sci. in History, Professor; simona23@bk.ru