# ОБЩИЕ ВОПРОСЫ ТЕОРИИ ПРАВА

**УДК 159.947** С. 8—14

## НЕКОТОРЫЕ СОЦИАЛЬНО-ЭКОНОМИЧЕСКИЕ ПРИЧИНЫ ДЕФОРМАЦИИ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА И ПРАВОВЫЕ СПОСОБЫ ИХ НЕЙТРАЛИЗАЦИИ[1]

**Пучков О. А.**
Уральский государственный юридический университет
E-mail: argun061@gmail.com.

В статье исследуются вопросы о различных формах деформаций в цифровой среде. Обращается внимание на появившиеся новые угрозы, производимые цифровой средой: человеческий капитал как главный фактор материальной экономики заменяется его цифровым дубликатом со многими проблемами в сфере производства и потребления, а также в сфере формирования менталитета. В статье акцентируется внимание на том, что «цифровая личность» сама становится объектом кражи и манипулирования со стороны хакеров. Делается вывод о том, что цифровая среда, предоставляющая, на первый взгляд, равенство возможностей для пользователей, тем не менее, приводит к «цифровому неравенству», с гораздо большим конфликтным потенциалом, чем материальный мир. В статье исследуются некоторые положения Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы и в этой связи делается вывод о невозможности создания глобальной системы информационной безопасности. Также обращается внимание на то, что действующие федеральные законы, предусматривающие вопросы регулирования безопасности в цифровой среде России, в основном носят не столько регулятивный, сколько доктринальный характер. В этой связи предлагается принять федеральный закон «О безопасном пользовании интернетом в Российской Федерации», который бы предусматривал повышение юридической ответственности пользователей сети.

**Ключевые слова:** информация, информационная среда, деформации цифровой среды, хакер, закон, киберпреступность, виртуальная экономика, виртуальные потребности, цифровая личность.

## SOME SOCIO-ECONOMIC REASONS DEFORMATION OF INFORMATION SPACE AND LEGAL METHODS OF THEIR NEUTRALIZATION

**Puchkov O. A.**
Ural State Law University
E-mail: argun061@gmail.com.

The article explores questions about various forms of deformations in a digital environment. Attention is drawn to the emerging new threats posed by the digital environment: human capital as the main factor in the material economy is replaced by its digital duplicate with many problems in the sphere of production and consumption, as well as in the formation of mentality. The article focuses on the fact that the "digital identity" itself becomes the object of theft and manipulation by hackers. It is concluded that the digital environment, which provides, at first glance, an equal opportunity for users, nevertheless, leads to a "digital inequality", with a much greater conflict potential than the material world. The article explores some of the provisions of the Strategy for the Development of the Information Society in the Russian Federation for 2017—2030,

[1] Исследование выполнено при поддержке Российского фонда фундаментальных исследований в рамках научного проекта № 18-29-16148 «Трансформация права в условиях развития цифровых технологий».

and in this regard, the conclusion is made about the impossibility of creating a global information security system. Attention is also drawn to the fact that the existing federal laws providing for the regulation of security in the digital environment of Russia are generally not so much of a regulatory as a doctrinal one. In this regard, it is proposed to adopt a federal law "On the safe use of the Internet in the Russian Federation", which would provide for an increase in the legal liability of network users.

**Keywords:** information, information environment, deformation of the digital environment, hacker, law, cybercrime, virtual economy, virtual needs, digital identity.

**Введение**

Проблема обеспечения безопасного «присутствия» человека в информационном пространстве приобрела последние два десятилетия острый характер. Все больше людей вовлекается в интернет-среду, все больше появляется новых технологий, которые с одной стороны, расширяют возможности делового оборота, общения, досуга людей, а с другой стороны, сама цифровая среда деформирует социально-экономический, психологический и правовой статус личности. В результате все больше появляется тех, кто стремится использовать «бреши» в обороне компьютеров, чтобы получить доступ к персональным данным пользователей и, в конечном счете, доступ к их финансам. Все это ставит с особой остротой проблему мер защиты от взлома компьютеров и правовых средств реагирования на эти вызовы. В данной статье предпринята попытка опираясь на данные о различных формах деформации информационного пространства, выявить некоторые причины этого явления и предложить правовые способы их нейтрализации.

**Методы**

В данном исследовании методы познания продиктованы реалиями цифрового мира. Такие явления, как цифровая личность, персональные данные, идентификация, электронная подпись, биометрические данные и другие объекты с виртуальной формой объективизации требует адекватного исследования с помощью методов теоретического исследования (восхождение от конкретного к абстрактному, синтез, позволяющие изучить объект в его целостности, единстве и взаимосвязи его частей. Оба эти метода близки к анализу, позволяющему верифицировать полученные в ходе исследования данные).

**Результаты**

Цифровой мир, представляющий собой особую область технологических, ментальных, социальных и иных взаимодействий — это новая среда обитания людей, обществ и государств, соразмерная по своей статусности с землёй, водой, воздухом, космосом. Вместе с тем, цифровой мир универсален, так как способен «впитывать» привычные для человека параметры бытия, основываться на них, управлять ими, а также создавать новые, неизвестные ранее: кибероружие, цифровой менталитет, киберугрозы, компьютерные «болезни» и прочую виртуальную реальность, даже не совместимую ни с какими объектами материального мира.

Материальный мир, легко поддающийся оцифровке, породил цифровой мир и стал от него повсеместно зависим. Тем не менее, отрыв виртуального мира от материального ещё не прошел точку невозврата, при которой социально-политические, экономические причины деформации информационного пространства станут не очевидными, а правовые способы их нейтрализации не действенными.

Пока у человечества есть некоторые возможности осознания этих причин и попыток их преодоления.

Итак, каковы социально-экономические причины деформации информационного пространства и какова динамика их развития?

Во-первых, виртуальная экономика построена на новых принципах и существенным образом отличается от принципов экономики материального мира: человеческий капитал материальной экономики заменяется его цифровым дубликатом, который является настоящим кладезем для манипулирования его потребностями и интересами вплоть до создания новых, не связанных с материальным миром и за которые «цифровая личность» готова заплатить. Так, например, 10 % людей носят одежду, подключенную к сети интернет, 10 % носят очки для чтения, подключенные к сети интернет, 90 % людей имеют возможность бесплатного и неограниченного хранения данных, имплантированных в мобильный телефон [1], медицина занимается созданием человеческих органов с использованием 3D печати, а цифровые симуляторы создают новые ощущения.

Таким образом, принцип человеческого капитала, действующий в материальной экономике, заменяется принципом индивидуально личностного капитала, в котором сама виртуальная личность может становиться объектом кражи, а её цифровые следы неуничтожимы.

Во-вторых, цифровая экономика создает свои «цифровые профессии», за которые цифровая личность получает пусть и в нематериальной форме, но вполне материальную оплату [6]. В то же время другие материальные профессии становятся ненужными, «вымываются» из материальной экономики и никак не включаются в цифровую в среду. За прошедший век численность людей, которые заняты в сфере производства товаров, необходимых обществу, снизились в разы: в странах — лидерах из 100 человек только двое работают в сельском хозяйстве, 10 — в промышленности, 13 — в управлении. Предполагается, что в России количество работников будет уменьшаться на 5 % ежегодно, и уровень безработицы через 3—4 года достигнет 20—25 % [1, с. 89].

В-третьих, цифровой менталитет, сформировавшийся у современной молодёжи, приводит к тому, что молодежь не живет в реальном экономическом пространстве, она играет «в жизнь» в киберпространстве. Как легко и безнаказанно кого-то убить цифровой игре, так легко и безнаказанно добыть в этой среде средства к существованию. Неравенство и деформации в социальном мире целиком восполняются равенством возможностей в цифровой среде, и молодежь этим активно пользуется. Так, К. Н. Евдокимов приводит данные статистики, о том, что возрастает количество несовершеннолетних преступников в цифровой среде, «их количество за разные годы составило от 20 до 60 %, то есть в среднем каждый третий» [5, с. 89]. Автор справедливо полагает, что среди потребностей социального характера на первое место выдвигаются самоутверждение, сохранение или повышение престижа, превосходство над окружающими, которые и формируют агрессивное поведение в цифровой среде. Развитие этих процессов будет, по нашему мнению, только усугубляться в связи с тем, что нивелирование высшего образования неизменно приводит к тому, что в результате технологического усложнения цифровой среды возникает другое неравенство с гораздо бóльшим конфликтным потенциалом — это неравенство в цифровой среде.

В-четвертых, коренным образом меняется потребление в цифровой экономике. Главными потребителями становится молодёжь, которую весьма условно можно подразделить по возрасту на две группы: 14—18 и 18—35 лет. В целом это около 40 миллионов человек. Разница здесь заключается не в интересах и потребностях, а лишь в возможностях и объемах их удовлетворения. Современное сетевое поколение переориентировалось на ценности нематериального характера-независимость, безответственность, неприкосновенность частной жизни. Это поколение «потребляет ради удовольствия, у него нет мотивации к длительному накоплению материальных ресурсов. Также у них снижена склонность к предпринимательскому риску» [10].

Понятие «потребление» деформируется, так как оно в виртуальном мире никак не связано с общественным производством. Возникает иллюзия, что 3D печать решает любые проблемы (при этом никак не делается акцент на то, что элементы 3D печати материальны и их тоже надо произвести).

В цифровом мире труд приобретает отчужденный характер и возникает особый чувственный потребительский фетишизм, когда за лайки в соцсетях идёт ежедневная борьба, на которую расходуется интеллектуальный ресурс сетевого поколения. Труд тоже в значительной мере видоизменился: он далеко не всегда целесообразен; он уже не при помощи орудий труда воздействует на природу, а в большей мере не воздействует на неё вообще; он не направлен чаще всего на создание предметов, удовлетворяющих сетевое поколение. Он направлен, как мы уже обращали внимание, на создание ощущений и потребление новых ощущений, создающихся в виртуальном пространстве. На это обращено особое внимание в «Стратегии развития информационного общества в Российской Федерации на 2017—2030 годы», в которой отмечается, что «темпы развития технологий, создания, обработки и распространения информации значительно превысили возможности большинства людей в освоении и применении знаний. Смещение акцентов в восприятии окружающего мира, особенно в сети Интернет, с научного, образовательного и культурного на развлекательно-справочный сформировало новую модель восприятия -так называемое клиповое мышление, характерной особенностью которого является массовое поверхностное восприятие информации. Такая форма освоения информации упрощает влияние на взгляды и предпочтения людей, способствует формированию навязанных моделей поведения, что дает преимущество в достижении экономических и политических целей тем государствам и организациям, которым принадлежат технологии распространения информации» [14]. В программном документе определен принцип

борьбы с этим негативным явлением в цифровой среде РФ — внедрение традиционных российских духовно-нравственных ценностей и соблюдение основанных на них норм поведения при использовании информационных и коммуникационных технологий. В этой связи возникает сомнение о реальном воплощении этого принципа, т. к. в п. 17 раздела II «Россия в современном информационном обществе» Стратегии особо отмечено, что никаких международно-правовых механизмов, позволяющих отстаивать суверенное право государств на регулирование информационного пространства, в том числе в национальном сегменте сети «Интернет» до сих пор не установлены. «Большинство государств вынуждены «на ходу» адаптировать государственное регулирование сферы информации и информационных технологий к новым обстоятельствам [14].

В-пятых, все возрастающее значение приобретает роль единичных акторов в цифровом мире и цифровой экономике в особенности, когда один хакер (или преступное их сообщество) в значительной мере могут воздействовать на вполне реальную, а не виртуальную экономику и политику государств. Киберпреступления становятся всё более непредсказуемыми (кража цифровых личностей, имитация биометрических данных и внешности человека. Покупка персональных данных с помощью Telegram-ботов и др.). Так в октябре 2019 г. специалисты Центробанка заявили, что за полгода обнаружили 13 000 объявлений о покупке и продаже персональных данных [3]. По данным Сбербанка РФ в 2019 году ущерб компаний от кибератак составил два с половиной триллиона долларов [2].

Ситуация на сегодняшний день такова, что пострадавшие от кибератак компании далеко не всегда обращаются за помощью в правоохранительные органы, так как выемка компьютеров или их блокировка в экономическом плане могут нанести серьезный экономический ущерб вдобавок к уже происшедшему.

В России, как и во всем мире не хватает специалистов по борьбе с киберугрозами. Ученые прогнозируют, что в 2021 г. будет 3,5 миллиона незакрытых вакансий в этой сфере на рынке труда [2].

В связи с тем, что информационные сети постоянно наполняются новым контентом, всё более и более нарастает информационная энтропия, которая губительно сказывается на экономических и социально-политических процессах в мире. Этому также способствует безответственность пользователей в цифровой среде. Так, Е. П. Ищенко отмечает, что «российские бизнесмены в принципе не желают тратится на дорогостоящие системы защиты от киберугроз и объяснение этому простое — большая часть их бухгалтерии — теневая и не фиксируется в электронной отчётности» [7, с. 33].

Каковы правовые возможности не противопоставить цифровую экономику материальной экономике, и не сделать ее конкурирующей с материальной? Эта война будет явно не в пользу последней. Предпринимаемые попытки по созданию системы кибербезопасности пока не приводят к успеху. Это связано с тем, что построить мировую систему безопасности невозможно в принципе (никто не отменял промышленный шпионаж и экономическую конкуренцию государств). Но даже если бы такая система и была бы создана, то это повлечет унификацию элементов этой системы, а любая унификация создает обратный эффект: большую вероятность ее взлома. В этой связи нам представляется более правильным решением обратить внимание законодателей не на глобальные процессы в Интернете, а на создание правовых условий для безопасного существования в интернете всех пользователей в Российской Федерации.

На наш взгляд, следует принять федеральный закон «О безопасном пользовании интернетом», в котором предусмотреть нормы об обязательных правилах, при соблюдении которых безопасность цифровой среды возрастает, а также предусмотреть ответственность пользователя за несоблюдение этих правил. Разумеется, такие акторы экономики как банки, компании могут вооружиться и дополнительными, специфическими для них способами защиты информации. Данный же закон должен распространяться на любых пользователей. Не надо забывать, что на сегодняшний день в онлайн находятся до 80 % россиян [17] и зачастую их простая невнимательность может нанести ощутимый урон экономическому статусу пользователей, а, следовательно, и экономике в целом. Это снижение покупательной способности, возрастание кредитной задолженности пользователей, утрата ими недвижимости и т. д.

По нашему мнению, следует обязать пользователей создавать уникальные пароли для каждой учетной записи. Согласно опросу, проведенному антивирусной компанией Avast, 55 % россиян используют один и тот же пароль для защиты нескольких учетных записей [17]. А это, безусловно, способствует киберпреступности, так как любой хакер попытается применить этот пароль во всех учетных записях. Также полагаем, что в законе следует прописать обязанность пользователей устанавливать и обновлять антивирусное программное

обеспечение. В Российской Федерации 48 % предприятий до сих пор используют устаревшие операционные системы [16], что само по себе создает угрозу их цифровой безопасности. В стране значительная часть компьютеров имеют устаревшую операционную систему Windows 7, а это, как правило, компьютеры с более чем семилетним сроком использования. «В январе 2020 года должна была закончиться поддержка операционной системы Windows 7. ОС перестанет получать обновления безопасности, что может поставить под угрозу сохранность данных компаний. При этом потери от инцидентов с данными могут оказаться выше, чем стоимость покупки новой ОС или компьютеров» [16].

Безусловно, Windows 10 более защищена: она снабжена многофакторной аутентификацией, предоставляет возможность новых способов авторизации, исключая пароли, в ней принудительно отключен протокол SMB 1, по которому в 2017 году работал вирус-вымогатель WannaCry, от которого пострадало «500 000 компьютеров, принадлежавших частным лицам, коммерческим организациям и правительственным учреждениям, в более чем в 200 странах мира. Экономический ущерб от этой атаки оценивается от 4 до 8 млрд долларов» [8]. Для определенных групп пользователей в законе следует прописать необходимость с установленной периодичностью обновлять операционную систему, адаптированной к новым угрозам в киберсреде (к примеру средствами биометрической аутентификации).

Следует установить запрет на осуществление переводов денежных средств для получения компенсаций, призов, пособий по ссылкам на определенные сайты, т. к. в 65 % всех случаев действует именно этот способ обмана в сети.

Немаловажным фактором борьбы, к примеру, с фишингом должен явиться запрет на тройную переадресацию, которая, как правило, приводит на сайт злоумышленников. Тактика киберпреступников состоит в «использование ссылок, ведущих на легитимные, но взломанные веб-сайты или к множественным переадресациям, которые кажутся безобидными, но в итоге приводят на фишинговые сайты» [15].

Также следует прописать в законе, в каких случаях возможнырасчеты в электронных валютах — биткоинах или альткоинах (например, только на основе смарт-контрактов или на основе децентрализации приложений). В тоже время здесь, безусловно, возникают трудности, так как поведение Bitcoin сложно поддается анализу в связи с тем, что оно «подкреплено минимумом реальных фактов» [4].

Важным фактором борьбы с различными видами преступлений в киберсреде будет установление запрета на требование отсылки по электронной почте ксерокопий паспортов и других персональных данных в тех сферах деятельности, где они не нужны. К примеру, широко известны случаи, когда управляющие компании при проведении собраний собственников жилья требуют от них предъявления ксерокопий паспортов, копий договоров купли-продажи жилья.

Также полагаем, что в целях предотвращения киберугроз следует по возможности создавать локальные информационные сети, не связанные с интернетом.

Таким образом, несмотря на реально возникшую необходимость создания Интернета-2, о котором много говорят специалисты, и в котором будут заложены всевозможные барьеры на пути киберугроз, а также попытки создания Рунета, пока даже не определили контуры борьбы с возникающими социально-экономическими угрозами в цифровой среде. По нашему мнению, чем более ответственным станет любой пользователь сети, чем выше будет у него уровень цифровой гигиены, тем устойчивее станут процессы противодействия нарастающему хаосу в цифровой среде. Пока же ситуация такова, что федеральные законы «Об информации, информационных технологиях и защите информации» [13], «О связи» [12], «О безопасности критической информационной инфраструктуры Российской Федерации» [11] не действуют в обозначенной нами сфере использования интернета. Они были заявлены, как справедливо отмечает Н. Е. Колобаева, как элементы механизма защиты права на распространение информации через сеть интернет. Эти законы призваны были создать условия для защиты российского сегмента в случае возникновения угрозы «со стороны» [9, с. 8].

Но возникает закономерный вопрос: где эта противоположная сторона в интернете? Как её можно установить, если Интернет пребывает вне границ и даже не во времени и не в пространстве. Он не уничтожим, даже если Землю постигнет Апокалипсис. Другой стороной может стать любой пользователь — как не знакомый с цифровой гигиеной и не несущий ответственность за неё, так и высочайший профессионал хакер (кракер).

На сегодняшний день весь механизм регулирования интернета со стороны государств состоит в блокировке вредоносных сайтов ив замедлении интернета с не четко определенным кругом субъектов, которые могут это инициировать и нести за это ответственность. Так, Роскомнадзор, выступающий ответчиком в таких делах, регулярно заявляет о том, что не является надлежащим ответчиком [9, с. 8].

**Выводы**

Всё вышесказанное делает очевидным факт, что только повышение ответственности пользователя в Российской Федерации уменьшит негативные последствия от многих выявленных нами угроз в цифровой среде, а принятие предложенного нами федерального закона станет наряду с другими нормативно-правовыми актами юридическим гарантом стабильности социально-экономических процессов в стране.

## Список литературы

1. Алиев, В. М. Политико-правовые аспекты перехода к цифровой экономике в России / В. М. Алиев // Российский следователь. — 2018. — № 9. — С. 48—52.

2. Безопасность в цифрах // РосБизнесКонсалтинг : [сайт]. — URL: http://win10pro.rbc.ru/article/bezopasnost-v-cifrax (дата обращения: 12.04. 2020).

3. В Роскачестве дали рекомендации по охране персональных данных в интернете // РосБизнесКонсалтинг : [сайт]. — URL: https://www.rbc.ru/rbcfreenews/5e2fd6c49a79479663914aa1 (дата обращения: 12.04. 2020).

4. Давыдов-Громадин Д. Ребром вверх. Как изменится цена Bitcoin в 2020 году / Д. Давыдов-Громадин // РосБизнесКонсалтинг : [сайт]. — URL: https://www.rbc.ru/crypto/news/ 5e3151b99a794731b96b0bd9 (дата обращения: 12.04. 2020).

5. Евдокимов, К. Н. Особенности личности преступника, совершающего неправомерный доступ к компьютерной информации (на примере Иркутской области) / К. Н. Евдокимов // Сибирский юридический вестник. — 2011. — № 1 (52). — С. 86—90.

6. Иванов, В. В. Цифровая экономика: мифы, реальность, перспектива / В. В. Иванов, Г. Г. Малинецкий. — Москва : Российская акад. наук, 2017. — 63 с.

7. Ищенко, Е. П. Виртуальный криминал / Е. П. Ищенко. — Москва : Проспект, 2014. — 232 с.

8. Киберпровалы, которые устраняются кнопкой «обновить» // РосБизнесКонсалтинг : [сайт]. — URL: http://win10pro.rbc.ru/article/kiberprovaly (дата обращения: 12.04. 2020).

9. Колобаева, Н. Е. Особенности реализации права на распространение информации в сети Интернет / Н. Е. Колобаева // Российское право: образование, практика, наука. — 2019. — № 4. — С. 4—10.

10. Новая боль экономики: молодежь не хочет потреблять как нормальные люди // Веб-агентство Текстерра : [сайт]. — URL: https://texterra.ru/blog/novaya-bol-ekonomiki-molodezh-ne-khochet-potreblyat-kak-normalnye-lyudi.html (дата обращения: 12.04. 2020).

11. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон № 187-ФЗ : от 26.07.2017 // Собрание законодательства РФ. — 2017. — № 31 (Части I—II). — Ст. 4736.

12. О связи : Федеральный закон № 126-ФЗ : от 07.07.2003 // Собрание законодательства РФ. — 2003. — № 28. — Ст. 2895.

13. Об информации, информационных технологиях и о защите информации : Федеральный закон № 149-ФЗ : от 27 июля 2006 г. // Российская газета. — 2006. — 29 июля.

14. Стратегия развития информационного общества в Российской Федерации на 2017—2030 годы : Указ Президента РФ : от 09.05.2017 № 203. // Собрание законодательства РФ. — 2017. — № 20. — Ст. 2901.

15. Тихая эволюция фишинга // РосБизнесКонсалтинг : [сайт]. — URL: http://win10pro.rbc.ru/article/fishing (дата обращения: 12.04. 2020).

16. Хайруллин, М. Переход к более быстрой и безопасной работе начинается с современного компьютера / М. Хайруллин // РосБизнесКонсалтинг : [сайт]. — URL: http://win10pro.rbc.ru/article/marat (дата обращения: 12.04. 2020).

17. Эксперты рассказали, как россиянам соблюдать безопасность в сети // АЭИ «Прайм» : [сайт]. — URL: https://1prime.ru/News/20200211/830921830.html (дата обращения: 12.04. 2020).

## References

1. Aliev, V. M. Politiko-pravovye aspekty perekhoda k tsifrovoy ekonomike v Rossii / V. M. Aliev // Rossiyskiy sledovatel. — 2018. — № 9. — S. 48—52.

2. Bezopasnost v tsifrakh // RosBiznesKonsalting : [sayt]. — URL: http://win10pro.rbc.ru/article/bezopasnost-v-cifrax (data obrashcheniya: 12.04. 2020).

3. V Roskachestve dali rekomendatsii po okhrane personalnykh dannykh v internete // RosBiznesKonsalting : [sayt]. — URL: https://www.rbc.ru/rbcfreenews/5e2fd6c49a79479663914aa1 (data obrashcheniya: 12.04. 2020).

4. Davydov-Gromadin D. Rebrom vverkh. Kak izmenitsya tsena Bitcoin v 2020 godu / D. Davydov-Gromadin // RosBiznesKonsalting : [sayt]. — URL: https://www.rbc.ru/crypto/news/ 5e3151b99a794731b96b0bd9 (data obra-shcheniya: 12.04. 2020).

5. Yevdokimov, K. N. Osobennosti lichnosti prestupnika, sovershayushche-go nepravomernyy dostup k kompyuternoy informatsii (na primere Irkutskoy oblasti) / K. N. Yevdokimov // Sibirskiy yuridicheskiy vestnik. — 2011. — № 1 (52). — S. 86—90.

6. Ivanov, V. V. Tsifrovaya ekonomika: mify, realnost, perspektiva / V. V. Ivanov, G. G. Malinetskiy. — Moskva : Rossiyskaya akad. nauk, 2017. — 63 s.

7. Ishchenko, Ye. P. Virtualnyy kriminal / Ye. P. Ishchenko. — Moskva : Prospekt, 2014. — 232 s.

8. Kiberprovaly, kotorye ustranyayutsya knopkoy «obnovit» // RosBiznesKonsalting : [sayt]. — URL: http://win10pro.rbc.ru/article/kiberprovaly (data obrashcheniya: 12.04. 2020).

9. Kolobaeva, N. Ye. Osobennosti realizatsii prava na rasprostranenie informatsii v seti Internet / N. Ye. Kolobaeva // Rossiyskoe pravo: obrazovanie, praktika, nauka. — 2019. — № 4. — S. 4—10.

10. Novaya bol ekonomiki: molodezh ne khochet potreblyat kak normalnye lyudi // Veb-agentstvo Teksterra : [sayt]. — URL: https://texterra.ru/blog/novaya-bol-ekonomiki-molodezh-ne-khochet-potreblyat-kak-normalnye-lyudi.html (data obrashcheniya: 12.04. 2020).

11. O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii : Federalnyy zakon № 187-FZ : ot 26.07.2017 // Sobranie zakonodatelstva RF. — 2017. — № 31 (Chasti I—II). — St. 4736.

12. O svyazi : Federalnyy zakon № 126-FZ : ot 07.07.2003 // Sobranie zakonodatelstva RF. — 2003. — № 28. — St. 2895.

13. Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite infor-matsii : Federalnyy zakon № 149-FZ : ot 27 iyulya 2006 g. // Rossiyskaya gazeta. — 2006. — 29 iyulya.

14. Strategiya razvitiya informatsionnogo obshchestva v Rossiyskoy Federatsii na 2017—2030 gody : Ukaz Prezidenta RF : ot 09.05.2017 № 203. // Sobranie zakonodatelstva RF. — 2017. — № 20. — St. 2901.

15. Tikhaya evolyutsiya fishinga // RosBiznesKonsalting : [sayt]. — URL: http://win10pro.rbc.ru/article/fishing (data obrashcheniya: 12.04. 2020).

16. Khayrullin, M. Perekhod k bolee bystroy i bezopasnoy rabote nachinaetsya s sovremennogo kompyutera / M. Khayrullin // RosBiznesKonsalting : [sayt]. — URL: http://win10pro.rbc.ru/article/marat (data obrashcheniya: 12.04. 2020).

17. Eksperty rasskazali, kak rossiyanam soblyudat bezopasnost v seti // AEI «Praym» : [sayt]. — URL: https://1prime.ru/News/20200211/830921830.html (data obrashcheniya: 12.04. 2020).

Дата поступления статьи в редакцию: 01.05.2020.