Правовое обеспечение международной информационной/кибер безопасности цифровой экономики: экономический и правовой аспекты

Получено: 08.10.2018; одобрено: 12.11.2018; опубликовано: 29.12.2018

УДК 341 JEL K240 DOI 10.26425/2658-3445-2018-2-61-66

Гонтарь Людмила Олеговна

Магистр, руководитель проекта «Knowledge+», Институт законодательства и сравнительного правоведения при правительстве Российской Федерации, Москва, Россия

e-mail: Cambridge.gontar@gmail.com

АННОТАЦИЯ

В статье рассмотрена проблема определения цифровой экономики, а также представлена новая тема относительно правового обеспечения международной информационной безопасности. Это новое направление служит показателем возможных междисциплинарных исследований в области права и экономики в сфере цифровых процессов. В качестве обоснования приведены акты Европейского союза и выделены их характерные черты, которые заключаются в анализе содержательной части цифровой экономики (экономической стороны). Это интеграционное объединение имеет уникальную структуру и историю, однако процесс регулирования цифровой экономики в Европейском союзе начался не так давно. Европейский союз – одно из немногих интеграционных объединений, которое начало заниматься работой по совершенствованию механизмов правового регулирования цифрового рынка. Это безусловно влияет на выработку комплексного подхода к понимаю цифровой экономики, а также еще в большей степени актуализирует вопрос правового обеспечения международной кибербезопасности исследуемого явления. Этот вопрос является новым направлением в международном правовом поле, которое позволит изучить востребованные правовые аспекты в цифровой экономике.

В статье проанализированы проблемы международной кибербезопасности и влияния понятийного аппарата на вопросы правового обеспечения безопасности цифровой экономики. Выработаны три предложения по совершенствованию подходов к безопасности цифровой экономики. По своей качественной характеристике предложения, касаются юридически-технических моментов, однако также представлены и решения относительно концептуальной составляющей правового обеспечения безопасности.

КЛЮЧЕВЫЕ СЛОВА

Цифровая экономика, правовое обеспечение международной кибербезопасности, акты Европейского союза, концепции, директивы, стратегии, информационный сегмент рынка, интеллектуальные системы, кибер-риски.

Legal procuring of international information/cyber security of the digital economy: economic and legal aspects

Recieved: 08.10.2018; aprobed: 12.11.2018; published: 29.12.2018

JEL classification K240 DOI 10.26425/2658-3445-2018-2-61-66

Gontar' Ludmila

Master of degree, project manager "Knowledge +", Institute of Legislation and Comparative Law at the Government of the Russian Federation, Moscow, Russia

e-mail: Cambridge.gontar@gmail.com

ABSTRACT

The article considers a problem of the definition of the digital economy, as well as presents a new theme on the legal procuring of international cyber security. The above mentioned new direction serves as an indicator of possible interdisciplinary research in the field of law and economics in the sphere of digital processes. As a justification the acts of the European Union have been adduced and their characteristic features, which consist in consideration of a substantial part of digital economy (economic party) have been allocated. This integration association has a unique structure and history, but the process of regulating the digital economy in the European Union began not so long ago. The European Union is one of the few integration associations that has started to work on improving the mechanisms of legal regulation of the digital market. This circumstance certainly affects the development of an integrated approach to the understanding of the digital economy, as well as further actualizes the issue of considering the legal procuring of international cyber security of this phenomenon. Legal procuring of security is a new direction in the international legal field, which will allow to consider the legal aspects in demand in the digital economy. The challenges in relation to international cyber security and the impact of the conceptual apparatus on the issues of the legal procuring of the security of the digital economy have been considered. It is important to note that the article suggests possible solutions to the problem posed. At the end of the article three proposals for improving approaches to the security of the digital economy have been elaborated. In terms of their qualitative characteristics, the proposals, undoubtedly, relate to legal and technical aspects, but also solutions regarding the conceptual component of the legal procuring of the security have been presented.

KEYWORDS

Digital economy, legal procuring of international cyber security, acts of the European Union, concepts, directives, strategies, informational segment of market, intellectual systems, cyber risks.

CITATION

Gontar' L.O. (2018). Legal procuring of international information/cyber security of the digital economy: economic and legal aspects. *E-Management*, vol. 1, № 2, pp. 61–66. DOI: 10.26425/2658-3445-2018-2-61-66

Актуальной темой исследований является цифровая экономика, а также процессы, происходящие в связи с ее развитием. Интересным представляется и вопрос правового обеспечения международной кибербезопасности цифровой экономики, так как аспекты безопасности в условиях формирования информационного общества являются обязательными компонентами укрепления стабильности цифровых отношений. Предпринималось множество попыток для определения понятия цифровой экономики. В своем послании Федеральному собранию Президент Российской Федерации В.В. Путин рекомендовал «…запустить масштабную системную программу развития экономики нового технологического поколения, так называемой цифровой экономики»[1]. В отчете парламента Великобритании обозначен весьма любопытный момент, касающийся природы цифровой экономики[2]. В отчете указано, что цифровая экономика одновременно сосредотачивает в себе предоставление материальных благ и информационный сегмент рынка. Существует множество заявлений и попыток детального рассмотрения цифровой экономики. Обратимся к некоторым доктринальным подходам с позиции экономической и юридической теории.

Первым, кто предложил данный термин с позиции экономической науки был Н. Негропонте [Negroponte N., 1995]. Связывался этот термин с интенсивным развитием информационно-коммуникационных технологий. Это наглядно прослеживается в связи с возникновением шестого технологического уклада, который охватывает все сферы экономической и социальной деятельности высокими технологиями и большими объемами информации. Основатель Media Labs Массачусетского технологического института Н. Негропонте, в середине 90-х гг. XX в. предсказавший возникновение цифрового мира, уже говорит о следующем десятилетии (20-х гг. XI в.) как о декаде биотехнологий. «Биотех – это новая «цифра», – утверждает он [Negroponte N., 1995, с. 256]. Если до сих пор искусственный и естественный миры развивались, то теперь они станут одним целым, пришло время их смешения.

Г. Валендук и П. Вендрамин [Valenduc and Vendramin, 2016] выделяют следующие принципы цифровой экономики, из которых и образуется определение. Цифровая экономика имеет четыре специфических принципа функционирования: оцифрованная информация становится стратегическим ресурсом государств; принцип «растущей отдачи» (нулевые издержки в процессе производства и т. д.); рост новых бизнес-моделей; промышленность 4.0, которая включает короткие производственные тиражи массово-ориентированных товаров, создание сетей производственной мощности. Это сопровождается размыванием границ между производителями, продавцами и потребителями [Valenduc and, Vendramin, с. 7–8].

Основатель Института актуального будущего О. Сальманов приводит любопытное сравнение экономики будущего (цифровой экономики) с человеком, выделяя три составляющие: плоть (электроника), кровь (связь), душа (люди)[3]. Отождествляет цифровую экономику с цифровой трансформацией всех аспектов человеческой деятельности. Фундаментальное исследование, проведенное М. Вогелсанг [Vogelsang, 2010] раскрывает причины возникновения цифровой экономики: цифровое развитие и интернет. Далее в исследовании раскрываются компоненты: сеть, информационно-технологический сервис, цифровые блага и другие смежные процессы.

Таким образом, в экономической литературе в большой мере обращают внимание на признаки, ресурсы цифровой экономики и изменения классических экономических законов.

С позиции юридической науки и практики также предпринимаются попытки дать определение или выделить основные черты цифровой экономики. Лучшие практики такой регламентации содержатся на уровне Европейского союза (далее – ЕС) в части выделения признаков этого явления. Именно эта международная организация посчитала возможным правовое регулирование в данной сфере. Заметим, что в большинстве актов ЕС отражается экономическая сущность регулируемых отношений, что позволяет говорить о синтезе правового, экономических и технических компонентов.

7 июля 2010 г. выходит директива ЕС «О структуре и развертывании интеллектуальных транспортных систем в области дорожного движения»[4]. В этой директиве отчетливо прослеживается специальный характер

[1] *«Парламентская газета»*, № 45, 02–08.12.2016. С. 2–3. Режим доступа: Справочная правовая система «КонсультантПлюс» http://www.consultant.ru/cons/ (дата обращения: 28.09.2018).

[2] *Counter-Extremism. Second Report of Session* 2016–17 (2016), P. 4–10. Режим доступа: https://publications.parliament.uk/pa/jt201617/jtselect/jtrights/105/105.pdf (дата обращения: 29.09.2018).

[3] *Экономика будущего* (2017). Издание ЦИПР по итогам конференции 24–26 мая 2017 г. Иннополис.

[4] *Directive 2002/21/EC of the European Parliament and of the Council of July 7,* (2010) “On a common regulatory framework for electronic communications

норм, направленных на обеспечение всех дорожных систем системой real-time, то есть, отображения ситуаций на дорогах в режиме реального времени и др. Самым важным является введение терминологического аппарата. Так, введены следующие термины: intelligent transport systems (определяется через проекцию дорожного и мобильного менеджмента), интероперабельность (означает способность систем и бизнес-процессов к обмену данными и информацией) и др. Всем государствам – членам ЕС надлежит применять меры для внедрения данных технологий посредством создания национального законодательства. Решение ЕС № 283, принятое в марте 2014 г., «О руководящих принципах для трансевропейских сетей в области телекоммуникационной инфраструктуры»[5] раскрывает преимущественно вопросы ширкополосных сетей по отношению к предыдущем директивам. Особенно интересен раздел «информационные интервенции (англ. digital interventions). Интервенции осуществляются исключительно в рамках внутреннего рынка ЕС и определяются как разовые услуги из частного сектора. Подобные действия имеют критерии, которые перечислены в документе (срок погашения и др.). Внесено предложение планирования долгосрочной устойчивости в информационной сфере. Решение № 910, принятое в июле 2014 г., «Об электронной идентификационных и доверительных услугах»[6] в условиях электронных транзакций и внутреннего рынка особенно подробно представляет понятийный аппарат. В документе прописывается соблюдение принципа внутреннего рынка, который выражается в следующем: не должно быть никаких ограничений по предоставлениям трастов, услуг на территории государства – члена ЕС; ограничений по продуктам и службам доверия, которые соответствовали настоящим правилам и имеется разрешение на распространение в пределах внутреннего рынка ЕС. Директива от 6 июля 2016 г. «О мерах по обеспечению высокого уровня безопасности сетевых и информационных систем через Евросоюз»[7] затрагивает организационные вопросы в части выполнения обязательств. Например, обязательство имплементировать национальную стратегию безопасности систем и информации. Было закреплено создание кооперативной группы (правовой статус не определен) для поддержки информационного обмена. В середине документа подводится итог, заключающийся в минимальной гармонизации, т. е. обмене информацией, технологиями, но не предоставление абсолютно всей информации. Рассматриваются термины: «национальная стратегия», «информационные системы», т. е. любое устройство или группа взаимосвязанных устройств, одна из которых выполняет автоматическую обработку или хранение цифровых данных, обрабатывает, извлекает или передает их в соответствии с целями эксплуатации, использования, защиты этих систем. Центральным звеном директивы является учреждение сети CSIRT (англ. computer security incident response team), т. е. сеть, состоящую из представителей данной сети государств − членов ЕС. Комиссия ЕС также участвует в сети в качестве наблюдателя. Эта сеть выполняет заданный обмен информацией об операционных службах и возможностях сотрудничества. По просьбе представителей этой сети от любого государства − члена ЕС может быть истребована информациях о рисках, информационном обмене и т. д. В директиве рассматривается и обязательство государств-членов по обеспечению организационных мер (мер, направленных на слаженные и регламентированные действия по обмену информацией и созданию единой нормативной базы либо во многом однородной между государствами-членами) управления рисками в отношении поставщиков цифровых услуг. В директиве прослеживается мысль о необходимости создания и в дальнейшем соблюдения единых стандартов по информационному обмену в сфере торговли и защите информации, новым технологиям, использующимся в секторах экономики киберзащиты. Имеется и новый термин, введенный по распоряжению Европейской комиссии, – «цифровой рынок Европы». Он предусмотрен документом «A digital single market strategy for Europe»[8] от 6 мая 2015 г. В документе имеются три опорных пункта, выступающие базисом цифрового рынка: доступ, под которым подразумеваются лучшие возможности доступа потребителей и бизнеса

networks and services". Режим доступа: https://eur-lex.europa.eu/homepage.html (дата обращения: 29.09.2018).

[5] *Regulation* (EU) No 283/2014 of the European Parliament and of the Council of March 11, 2014 "On guidelines for trans-European networks in the area of telecommunications infrastructure" and repealing Decision № 1336/97/EC. Режим доступа: https://eur-lex.europa.eu/homepage.html (дата обращения: 28.09.2018).

[6] *Regulation* (EU) № 910/2014 of the European Parliament and of the Council of July 23, 2014 "On electronic identification and trust services for electronic transactions in the internal market" and repealing Directive 1999/93/E. Режим доступа: https://eur-lex.europa.eu/homepage.html (дата обращения: 29.09.2018).

[7] *Directive* (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 "Concerning measures for a high common level of security of network and information systems across the Union". Режим доступа: https://eur-lex.europa.eu/homepage.html (дата обращения: 23.12.2018)

[8] *Press release for Europe "Commission sets of 16 initiatives to make it happen"*. Brussels. May 6, 2015. Режим доступа: https://eur-lex.europa.eu/homepage.html (дата обращения: 22.09.2018).

на территории Европы; инфраструктура и управление (среда), т. е. создание единых правовых условий и равных конкурентных возможностей для новых сетей инновационных проектов; экономика и общество, т. е. максимизация потенциала роста цифровой экономики.

Наиболее междисциплинарным проектом в рамках ЕС является создание индекса DESI (Digital economy and society index)[9] в 2017 г. Он состоит из суммы следующих показателей: связи; человеческого капитала; использования Интернета; интеграции цифровых технологий; технических центров. Эти показатели целиком состоят из графических и числовых показателей, которые сравнивают характеристики «информационности» каждой из стран – участниц ЕС. Индекс дает возможность определить, насколько быстро внедряются информационные технологии.

Итак, исходя из сжатого экономического и правового анализа признаков, компонентов и характерных свойств, можно сделать вывод, что цифровая экономика – это осложненный техническими характеристиками вариант развития производственных отношений, имеющий характер трансграничности, регулируемый исключительно с помощью международного права посредством актов международных организаций. Цифровая экономика в рамках ЕС – показательный пример того, что на международном уровне нужен постепенный процесс выработки единого определения цифровой экономики. Разумеется, помимо выработки самого определения, исходя из анализа литературы по экономической теории, безусловно требуется решить наиболее практический вопрос относительно правового обеспечения международной кибербезопасности цифровой экономики. Подобные правовые действия, на наш взгляд, более чем необходимы для надлежащего оформления в нормативно-правовой базе отношений в сфере цифровой экономики. Дело в том, что абсолютно все аспекты экономических отношений урегулировать нельзя, потому полагаем, что аспект международной безопасности является эффективным, и его правовое обеспечение (закрепление в нормативной базе и осуществление действий по реализации правовых положений) может послужить неплохим началом для легализации цифровой экономики и процессов, связанных с ней, в правовой системе.

Международная кибербезопасность представляет собой состояние защищенности субъектов международного права, отношений между ними в международном киберпространстве с целью поддержания мира и недопущения ведения войн при помощи технологических новшеств. Если рассматривать этот вопрос с учетом нашей позиции, возникает разделение на два аспекта:

1) современное компьютерное оснащение, вирусы, информационные данные, а также модификации кибероружия, которые можно использовать для подрыва мира и безопасности вне виртуального пространства;

2) виртуальное пространство само может стать местом военных конфликтов и подрыва международной безопасности.

Мы полагаем, что концентрация внимания на аспект безопасности, как в правовом, так и содержательном смысле, будет надлежащим образом способствовать стабилизации отношений в цифровой экономике. В связи с этим следует говорить о необходимости формулировки концепции правового обеспечения международной кибербезопасности цифровой экономики. Будет верным обратиться к документам на международном уровне, таким как акты Международного союза электросвязи, так как именно данный субъект международных отношений рассматривает проблему кибербезопасности на высоком количественном и качественном уровнях, например, к докладу «Глобальный индекс кибербезопасности»[10], подготовленный Группой кибербезопасности (подразделение Международного союза электросвязи). Этот индекс представляет собой усовершенствованную эталонную модель, которая состоит из 25 показателей, целью которой является сравнение уровня обязательств государств − членов Международного союза электросвязи в области кибербезопасности. Основными задачами данного индекса выступают: определение типа, уровня и эволюции обязательств в области кибербезопасности в странах; обязательства по преодолению разрыва в кибербезопасности и определению различий и др. Генеральный директор Международного союза электросвязи Б. Саноу[11] пишет о том, что этот индекс используют в качестве ключевого фактора, способствующего экономическому развитию. Также он подчеркивает, что правительства во всем мире признают, что преобразование по информационным технологиям сильно влияет на благополучие граждан. Кибербезопасность, по его словам, должна быть неотъемлемой и неделимой частью технического прогресса.

---

[9] *Foley P., Sutton D., Wiseman I., Green L. and Moore J.* (2018). International Digital Economy and Society Index 2018 SMART 2017/005.2018. Режим доступа: https://eur-lex.europa.eu/homepage.html (дата обращения: 24. 09.2018).

[10] *Global Cybersecurity Index* (GCI) (2017). Режим доступа: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (дата обращения:02.09.2018).

[11] Там же.

Глобальный индекс кибербезопасности базируется на нескольких элементах. Условно выделим значимые для нас: правовой (отражение в правовых нормах кибербезопасности), технический (технологические компоненты и механизмы), организационный (разработка стратегий и прочей системы мер по реализации кибер-защиты). Подбор данных осуществляется посредством консультаций с группой экспертов. Опрос проводится через онлайн-платформу, через которую собираются статистические данные. Также индекс содержит свою собственную методологию, состоящую из 25 показателей и 157 вопросов. Показатели вырабатываются основании таких критериев, как актуальность, наличие и качество данных, возможность перекрестной проверки через вторичные данные. Глобальный индекс кибербезопасности не просто выполняет роль какого-то статистического документа, но содержит попытки постепенной стабилизации отношений в сфере кибербезопасности и попытки выработки стратегий борьбы с некоторыми глобальными угрозами в данной сфере.

Попытка анализа и проецирования (более углубленно) на процессы, происходящие в связи с цифровой экономикой позволит сделать первые стадии правового обеспечения международной кибербезопасности цифровой экономики более оперативными и в определенной степени позволит предупредить кибер-риски. Последние понимаются как вирусные угрозы, внедрение вредного программного обеспечения, эксплойты инфраструктуры, хищение информации, дезинформация на рынке услуг цифровой экономики и др.

Предлагаем следующие последовательные пункты первых стадий развития правового обеспечения международной кибербезопасности цифровой экономики.

1. Разработать программный документ по цифровой экономике, позволяющий определить основные характеристики данного явления.
2. Рассмотреть вопрос относительно последовательности направлений цифровой экономики и аспектов ее безопасности. Важно отметить, что документ не должен включать лишь общее определение безопасности, а наоборот, рассмотреть общие и специальные признаки безопасности цифровой экономики. Возможно следует исследовать это явление сквозь призму международных и национальных актов, которые рассматривают понятие кибербезопасности и спроецировать основные компоненты данной концепции на условия отношений в цифровой экономике. Это позволит трансформироваться концептуальным началам правового обеспечения с учетом кейсов по цифровой экономике и стать более практичными и эффективными в использовании.
3. Определить компетентный орган / группу органов, которые будут заниматься специальным регулированием правового обеспечения международной кибербезопасности цифровой экономики.

Таким образом, исходя из вышесказанного можно сделать вывод, что, безусловно, понятийный аппарат цифровой экономики и процессы, связанные с ней, нуждаются в правовом обеспечении международной кибербезопасности. Однако данный процесс должен быть надлежащим образом изучен как в экономической, так и в юридической доктрине, а также апробирован на практике для эффективной оценки результата.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Negroponte N. (1995). Being Digital. NY.: Knopf.

Valenduc G., Vendramin P. (2016). Work in the digital economy: sorting the old from the new. European trade union institute. Pp. 7–8.

Vogelsang M. (2010). Digitalization in Open Economies. Theory and Policy Implications. Springer-Verlag Berlin Heidelberg.

REFERENCES

Negroponte N. (1995). *Being Digital*, NY.: Knopf.

Valenduc G. and Vendramin P. (2016). *Work in the digital economy*. European trade union institute. Pp. 7–8.

Vogelsang M. (2010). *Digitalization in Open Economies*. Theory and Policy Implications. Springer-Verlag Berlin Heidelberg.