

# ПРАВО И ИНФОРМАЦИЯ:

ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ

gov.ru duma.gov.ru ksrf.  
cremlin.ru  
b.ru kremlin.ru minsvyaz.ru m  
orf.ru gosuslugi.ru minjus  
ru mil.ru mvd.ru genproc.gov.ru  
mlin.ru gov.ru duma.  
u gosuslugi.ru minjust.ru  
nvd.ru genproc.gov.ru fsb.ru  
ma.gov.ru ksrf.ru U  
n.ru  
mlin.ru minsvyaz



СБОРНИКИ ПРЕЗИДЕНТСКОЙ БИБЛИОТЕКИ

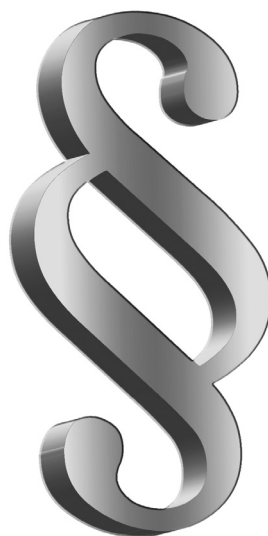
Серия «Электронное законодательство»

*Выпуск 6*

---

# ПРАВО И ИНФОРМАЦИЯ: ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ

Сборник материалов  
международной научно-практической конференции



Санкт-Петербург  
Президентская библиотека  
2017

УДК 340  
ББК 67.401.114я43  
ББК 67.404.31я43

Научный редактор:  
*Н. А. Шевелёва*, д-р юрид. наук, профессор, СПбГУ

Редакционная коллегия:  
*Н. В. Дунаева*, д-р юрид. наук, профессор, *К. Н. Княгинин*, канд. юрид. наук,  
*Д. А. Савельев*, канд. юрид. наук, Президентская библиотека;  
*В. Б. Наумов*, канд. юрид. наук, доцент, СПбГУ, компания Dentons

Рецензент:  
*В. В. Мамонов*, д-р юрид. наук, профессор, ГАОУ ВО Ленинградской области  
«Ленинградский государственный университет им. А. С. Пушкина»  
Серия «Электронное законодательство». Основана в 2011 г.

**Президентская библиотека имени Б. Н. Ельцина (Санкт-Петербург)**

Сборники Президентской библиотеки / Президент. б-ка им. Б. Н. Ельцина. – СПб. : Президентская библиотека, 2011 – .

Серия «Электронное законодательство». – 2011.

Вып. 6 : Право и информация: вопросы теории и практики : сб. матер. междунар. науч.-практ. конф. / Науч. ред. Н. А. Шевелёва, д-р юрид. наук, проф. – 2017. – 235 с.

ISBN 978-5-905273-88-9

В сборнике опубликованы материалы международной научно-практической конференции «Право и информация: вопросы теории и практики», проведенной 15 апреля 2016 г. ФГБУ «Президентская библиотека имени Б. Н. Ельцина».

Материалы, представленные в выпуске, сгруппированы в два раздела. Специальный раздел сборника посвящен перспективным направлениям совершенствования законодательства, прежде всего, об интеллектуальных правах, применительно к сфере доступа к информации в библиотеках. Во втором разделе собраны материалы, относящиеся к совершенствованию информационного права, в частности, регулирования обращения с персональными данными, деятельности СМИ, а также к вопросам правовой информатики.

В приложении к сборнику представлены материалы виртуальной выставки «Из истории развития российского законодательства о печати».

УДК 340  
ББК 67.401.114я43  
ББК 67.404.31я43

- © ФГБУ «Президентская библиотека имени Б. Н. Ельцина», 2017  
© Коллектив авторов, 2017

Электронная версия настоящего издания является свободно распространяемой. Любое лицо вправе безвозмездно воспроизводить и доводить до всеобщего сведения в электронной форме настоящее издание на весь срок охраны авторского права и на территории всего мира при условии некоммерческого характера использования, сохранения целостности всего издания, указания имен авторов, первоначального адреса публикации [www.rplib.ru](http://www.rplib.ru) и данного текста условий. Осуществление указанных действий означает принятие настоящих условий.

ISBN 978-5-905273-88-9

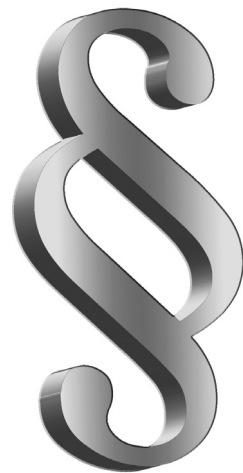
PRESIDENTIAL LIBRARY COLLECTIONS

"Electronic Legislation" Series  
*Issue 6*

---

# LAW AND INFORMATION: THE QUESTIONS OF THEORY AND PRACTICE

Collection of works of international  
scientific and practical conference



St. Petersburg  
The Presidential Library  
2017

Scientific Editor  
Prof. Dr. *Natalya A. Sheveleva*, St. Petersburg State University

Editorial Board:  
Prof. Dr. *Natalya V. Dunaeva*, Dr. *Konstantin N. Knyagin*,  
Dr. *Denis A. Saveliev*, Presidential Library;  
Dr. *Victor B. Naumov*, St. Petersburg State University, Dentons

Reviewer:  
Prof. Dr. *Vadim V. Mamonov*,  
Pushkin Leningrad State University

Translated by *Denis A. Saveliev*  
Proofreader of the English version *Anna D. Barkhatova*

“Electronic Legislation” Series  
Established in 2011

**The Boris Yeltsin Presidential Library (St. Petersburg)**

The Presidential Library Collections. St. Petersburg: The Boris Yeltsin Presidential Library, 2011 – .

“Electronic Legislation” Series. – 2011.

Issue 6 : Law and Information: The Questions of Theory and Practice /  
Scientific Editor Prof. Dr. Natalya A. Sheveleva. – 2017. – 235 p.

ISBN 978-5-905273-88-9

In the issue the papers of international scientific and practical conference “Law and Information: The Questions of Theory and Practice” held on April, 15, 2016 by Presidential Library are published.

The topics of the issue are grouped into two chapters. A special chapter is devoted to the development of legislation on access to information in libraries, especially on copyright. The second chapter is devoted to the development of information law, especially personal data regulation, mass media and information technologies regulation related to legal data.

In the addition the virtual exhibition “On the History of Russian Legislation on Press” is presented.

- © The Boris Yeltsin Presidential Library, 2017
- © Authors, 2017

The electronic copy of the present issue is redistributable free of charge. Any person has the right to make electronic copies and distribute the present issue in electronic form within the entire term of the copyright protection and worldwide on non-commercial basis, retaining the integrity of the issue, author’s names, original publication address [www.prlib.ru](http://www.prlib.ru) and this license text. Using this right means the acceptance of the terms and conditions.

**ISBN 978-5-905273-88-9**

## Содержание

<i>Список используемых сокращений</i> .....	16
<b>Шевелёва Н. А.</b> Введение .....	17

### Часть I

#### Авторское право и электронные библиотеки

<b>Ван Чжукан.</b> О проблемах применения авторского права, возникающих при создании публичной библиотекой баз данных .....	20
<b>Гуляева Н. С.</b> Авторское право в информационном обществе: вызовы и возможности для библиотек .....	38
<b>Кулаков Н. А., Савельева М. В.</b> Административная ответственность как способ защиты авторских и смежных прав на литературные произведения, опубликованные в электронных библиотеках в сети Интернет.....	44
<b>Рузакова О. А.</b> Проблемы развития законодательства об интеллектуальных правах в библиотечном деле .....	49
<b>Савельев Д. А.</b> Информация, документ, произведение: исследование соотношения понятий в информационном праве, интеллектуальных правах, а также в законодательстве о библиотечном деле.....	56

## Часть 2

### Информационное право и правовая информатика

<b>Агеева Е. В., Самовольцева К. А.</b> Информационно-аналитическое обеспечение государственных органов власти и управления: опыт работы Президентской библиотеки Республики Беларусь.....	62
<b>Али М. З.</b> Ответственность владельца интернет-сайта как информационного посредника.....	67
<b>Аристархов А. Л.</b> Тенденции применения электронных технологий в уголовно-процессуальной деятельности.....	72
<b>Бражник Т. А.</b> Многосторонний подход к сетевой нейтральности.....	83
<b>Булгакова Е. В.</b> Методы анализа больших данных в решении юридических задач .....	90
<b>Виткова Л. А., Рябова О. Н., Сахаров Д. В.</b> Открытые данные как единая составляющая механизма реализации стандарта открытости государства .....	97
<b>Вильчинская Э. А., Виткова Л. А., Парсон И. М.</b> Актуальные проблемы правового регулирования средств массовой информации.....	102
<b>Вус М. А., Юсупов Р. М.</b> К вопросу о Модельном законе Организации Договора о коллективной безопасности «О государственной тайне» ...	109
<b>Григорьев А. А., Охрименко А. А., Сидорчук И. П.</b> Обеспечение отдельных прав при формировании информационного общества .....	116
<b>Дорский А. Ю.</b> Практика применения «Закона о блогерах» .....	124
<b>Домрачев А. А., Исаков В. Б., Фургель И. А.</b> Формирование единых региональных цифровых пространств с использованием трансграничного пространства доверия .....	129
<b>Журавлев М. С.</b> Защита персональных данных в телемедицине.....	151

# Формирование единых региональных цифровых пространств с использованием трансграничного пространства доверия

*А. А. Домрачев, В. Б. Исаков, И. А. Фургель\**

*Формирование единых региональных цифровых пространств (ЕЦП) в рамках глобальной экономики является актуальным трендом современности и нацелено на обеспечение условий для ускоренной интеграции и развития различных региональных объединений как эффективной и конкурентоспособной организации в рамках мировой экономики, а также для устойчивого развития экономик отдельных стран в интересах повышения жизненного уровня их населения. В статье предлагаются концептуальные подходы к построению архитектуры ЕЦП.*

**Ключевые слова:** информационное пространство, Интернет, экономика, блокчейн.

## Общие архитектурные решения

**Мотивация.** Проникновение цифровых и информационно-коммуникационных технологий (далее – ИКТ) в различные отрасли экономики и промышленности, деятельность органов государственной власти и управления, а также в повседневную жизнь граждан является глобальной тенденцией в мировом масштабе и в полной мере относится к развитым и развивающимся странам.

Происходящие технологические сдвиги приводят к формированию национальных и региональных стратегий и программ, направленных на

---

\* *Домрачев Алексей Александрович*, советник Департамента проектов по информатизации Министерства связи и массовой коммуникации Российской Федерации; *Исаков Владимир Борисович*, доктор юридических наук, профессор Национального исследовательского университета «Высшая школа экономики». visakov@hse.ru; *Фургель Игорь Аркадьевич*, Dr. rer. nat., руководитель органа подтверждения и сертификации T-Systems International GmbH.



создание единых цифровых пространств в условиях фактически происходящего перехода к цифровой экономике.

Формирование ЕЦП в рамках глобальной экономики является актуальным трендом современности и нацелено на обеспечение условий для ускоренной интеграции и развития различных региональных объединений как эффективной и конкурентоспособной организации в рамках мировой экономики, а также для устойчивого развития экономик отдельных стран в интересах повышения жизненного уровня их населения.

Например, бизнес-сообщество стран Евразийского экономического союза предложило сформировать единое цифровое пространство ЕАЭС. Такая идея была выдвинута на прошедшем в ноябре 2015 г. в Минске первом заседании президиума Делового совета ЕАЭС.

Члены совета отметили, что решение поставленных перед ЕАЭС задач по укреплению экономик государств-членов, обеспечению их гармоничного развития и сближения, устойчивому росту деловой активности, сбалансированности торговли и добросовестной конкуренции может быть ускорено за счет консолидации усилий по реализации совместных программ и проектов по цифровой трансформации и формированию единого цифрового пространства ЕАЭС<sup>1</sup>.

Аналогичные тенденции отмечаются в европейском (проект eIDAS<sup>2</sup>) и азиатско-тихоокеанском (проект Паназиатского альянса по электронной коммерции<sup>3</sup>) регионах.

Условно выделяются три базовых процесса формирования ЕЦП:

- цифровая трансформация государственного управления, охватывающая использование цифровых технологий в предоставлении услуг, информационном обмене между государственными органами, бизнесом и гражданами, надзоре, основанном на оценке рисков;
- формирование цифрового рынка, включающее обеспечение свободного и беспрепятственного доступа в Интернет товаров и сервисов, услуг капитала, в том числе электронные деньги, физических и юридических лиц в условиях справедливой конкуренции, при высоком уровне защиты их законных прав и персональных данных, независимо от места их жительства, гражданства и места совершения сделки;
- цифровая трансформация экономики, подразумевающая цифровую трансформацию традиционных отраслей экономики, возникновение новых цифровых отраслей товаров и услуг, и носящая общее название «индустрия 4.0».

---

<sup>1</sup> URL: <http://www.e-cis.info/news.php?id=13561>

<sup>2</sup> URL: <https://ec.europa.eu/digital-single-market/en/trust-services-and-eid>

<sup>3</sup> URL: <https://paa.net/>

Сложность процессов, происходящих во многих развитых и развивающихся странах, их значимость, которая закрепляется в соответствующих документах, а также заложенный в них потенциал модернизации экономики, совершенствования бизнес-среды и увеличения роста объемов взаимного оборота товаров, услуг, капитала и рабочей силы требуют все более пристального изучения и включения в повестку практических задач на ближайшие годы, налаживания скоординированных действий стран в этой сфере. Например, в Европейском союзе формирование цифрового единого рынка включено в число его десяти приоритетов.

Многие проблемные вопросы, связанные с формированием ЕЦП, обусловлены недостаточной развитостью нормативной правовой базы в условиях бурного роста применения ИКТ во всех сферах регулирования. В результате в недостаточной степени используется потенциал электронной торговли для расширения товарооборота между странами, гармонизации систем электронного правительства, предоставления гражданам и хозяйствующим субъектам межгосударственных юридически значимых электронных услуг, налаживания отраслевых кооперационных связей.

Использование ИКТ как инструмента для ускорения и развития интеграционных процессов пока еще носит фрагментарный, а не системный характер. Недостаточно учитывается, что большинство интеграционных процессов в значительной степени связано с необходимостью налаживания эффективного, в том числе юридически значимого информационного взаимодействия на базе формирования совместно используемых информационных ресурсов.

Указанные тенденции будущего развития показывают необходимость и своевременность максимального использования потенциала различных интеграционных проектов и объединения усилий стран в рамках движения к цифровой трансформации своих экономик и построению ЕЦП.

**Концептуальные подходы.** Решение поставленных в странах стратегических задач по укреплению экономик, обеспечению их гармоничного развития и сближения, устойчивого роста деловой активности, сбалансированности торговли и добросовестной конкуренции может быть ускорено за счет консолидации усилий по реализации совместных программ и проектов по формированию ЕЦП. В этой связи задача формирования ЕЦП становится ключевой и центральной для перспективного развития мировых интеграционных процессов как в направлении «углубления», так и «расширения» в глобальном мировом экономическом пространстве.

При подготовке долгосрочных стратегических ориентиров по формированию ЕЦП следует учитывать мировые тенденции в этой области, в том числе опыт соответствующих институтов в Европейском Союзе. Так, например, в Цифровой повестке дня Европы в рамках Стратегии Европы 2020 г. предусмотрены следующие основные направления развития:

- улучшение доступа потребителей и бизнеса к цифровым технологиям приобретения товаров и услуг;
- формирование условий для развития инфраструктуры цифровых сетей и услуг;
- создание цифровой экономики и цифрового общества с долгосрочным потенциалом роста.

Перечисленные направления в полной мере актуальны и для других регионов мира. При этом приоритетными практическими работами при формировании ЕЦП могут стать:

- развитие нормативной правовой базы отдельных стран и их гармонизация для целей формирования ЕЦП и цифровой трансформации экономик;
- формирование ЕЦП как одного из основных каналов для увеличения взаимного товарооборота с использованием инструментов электронной торговли;
- расширение практики использования ИКТ для повышения эффективности, в том числе юридической, трансграничного взаимодействия между государственными органами, хозяйствующими субъектами и физическими лицами;
- разработка и реализация совместных проектов и программ, направленных на цифровую трансформацию экономик стран;
- формирование электронных сервисов по направлениям «четырёх свобод» – перемещения товаров, услуг, капитала и рабочей силы.

Содержательная схожесть задач по формированию ЕЦП в различных регионах мира и необходимость их последующей интеграции в рамках глобальной экономики актуализируют проблему выработки базовых архитектур цифровой экономики на основе имеющегося опыта, полученного прежде всего в рамках Центра ООН по упрощению процедур торговли и электронным деловым операциям (СЕФАКТ ООН), в том числе по темам формирования и функционирования единого окна и трансграничного пространства доверия, как естественное развитие указанных тем в направлении ЕЦП.

Задача по реализации мероприятий по формированию ЕЦП Евразийского экономического союза уже выдвинута на повестке дня, что также предполагает выработку базовых архитектур.

При построении архитектуры ЕЦП мы предлагаем следующие концептуальные подходы.

В рамках верхнего уровня необходимо выделить набор решений *инфраструктурного* и *функционального* характера. Функциональные решения предназначены для непосредственного удовлетворения различных общественных потребностей экономического и социального характера, тогда как

инфраструктурные решения нацелены на придание функциональным сервисам определенных свойств/качеств, таких, как доверие и безопасность<sup>1</sup>.

Таким образом, функциональные и инфраструктурные решения являются дополнительными по отношению друг к другу и поэтому должны рассматриваться и проектироваться всегда в комплексе.

*Функциональные* решения могут быть такими же разнообразными и многоцелевыми, как и сама жизнь, так как они служат удовлетворению всевозможных общественных и социальных потребностей. К решениям *функционального* характера можно отнести:

- концентраторы (хабы) сервисов электронной коммерции<sup>2</sup>;
- электронные платежные системы;
- системы предоставления электронных государственных услуг;
- системы телемедицины;
- системы дистанционного образования;
- системы единого окна<sup>3</sup>;
- различные приложения: Internet of Things (IoT)<sup>4</sup>, умный дом, smart город, Internet of Vehicles (IoV)<sup>5</sup> и др.;
- различные информационно-аналитические системы в совокупности с системами маркировки товаров, предназначенные в том числе для мониторинга товарных потоков, который может осуществлять конечный потребитель.

К решениям *инфраструктурного* характера, включающим также аспекты информационной безопасности, необходимо отнести:

- региональные и глобальные трансграничные пространства доверия (ПД-Т)<sup>6</sup>;
- системы защиты персональных данных<sup>7</sup>;
- системы защиты коммерческой тайны;
- другие решения, в том числе информационно-безопасные, вносящие вклад в достижение и сохранение необходимого уровня доверия между пользователями соответствующей инфраструктуры.

**Архитектурные решения.** Важным архитектурно образующим признаком ЕЦП является целесообразность использования трансграничного пространства доверия (ПД-Т) для поддержки юридически значимого

---

<sup>1</sup> Безопасность является одним из аспектов доверия.

<sup>2</sup> URL: <http://paa.net/>

<sup>3</sup> URL: [https://en.wikipedia.org/wiki/Single-window\\_system](https://en.wikipedia.org/wiki/Single-window_system); URL: [http://www.unece.org/fileadmin/DAM/trade/ctied7/ece\\_trade\\_324e.pdf](http://www.unece.org/fileadmin/DAM/trade/ctied7/ece_trade_324e.pdf)

<sup>4</sup> URL: [https://en.wikipedia.org/wiki/Internet\\_of\\_Things](https://en.wikipedia.org/wiki/Internet_of_Things)

<sup>5</sup> URL: [http://mddb.apec.org/Documents/2014/TEL/TEL50-PLen/14\\_tel50\\_plen\\_020.pdf](http://mddb.apec.org/Documents/2014/TEL/TEL50-PLen/14_tel50_plen_020.pdf)

<sup>6</sup> URL: <http://www1.unece.org/cefact/platform/download/attachments/55378391/Rec+draft+v.0.952+10.03.16.pdf>

<sup>7</sup> URL: <http://www.cbprs.org/Consumers/ConsumerDetails.aspx>

трансграничного электронного документооборота в рамках любых функциональных сервисов, требующих либо предполагающих определенный уровень доверия между пользователями этих сервисов.

Это в особенности относится к функциональным решениям, которые можно отнести к классу учетных информационных систем. В них содержится информация из правоустанавливающих документов, которая требует специальных мер поддержки со стороны электронных сервисов *доверия*. К таким функциональным приложениям относятся, например, юридически значимые услуги, предоставляемые на основе концентраторов (хабов) электронной коммерции, электронные платежные системы, а также системы предоставления электронных государственных услуг, телемедицины, дистанционного образования и единого окна.

Под ПД-Т мы понимаем совокупность правовых, организационных и технических условий, рекомендуемых специализированными структурами ООН и профильными международными организациями с целью обеспечения доверия при международном обмене электронными документами и данными между субъектами электронного взаимодействия.

Под субъектами электронного взаимодействия мы понимаем органы государственной власти, физические и юридические лица, взаимодействующие в рамках отношений, возникающих при формировании, отправке, передаче, получении, хранении и использовании электронных документов и данных.

Создание и сохранение общих предпосылок для установления и поддержания определенного (требуемого или ожидаемого) уровня доверия между субъектами электронного взаимодействия с целью обеспечения взаимного юридически значимого признания сервисов доверия, предоставляемых под различными юрисдикциями, является *системообразующим фактором* ПД-Т.

Необходимо подчеркнуть, что «доверие» само по себе является фундаментально общественной функцией. Поэтому построение какого-либо института, обеспечивающего «доверие» и одновременно основанного исключительно на технологиях, а не на общественных отношениях, представляется невозможным.

Эффективным путем обеспечения доверия в рамках ПД-Т видится сопряжение традиционно существующих институтов, способных адекватно поддерживать реализацию системообразующего фактора ПД-Т, с организационными и технологическими возможностями, предоставляемыми современными ИКТ-сервисами.

Отдельные функциональные приложения, такие, например, как процедуры урегулирования споров в режиме онлайн, могут не использовать весь инструментарий ПД-Т, а только упрощенные специфические системы идентификации истцов, ответчиков и третьих сторон, адекватные тем, что используются на тех торговых площадках, где возник спор.

Различные функциональные приложения, такие, как Internet of Things (IoT), умный дом, смарт-город, Internet of Vehicles (IoV) и другие аналоги можно отнести к классу информационно-справочных систем, которые обрабатывают различную информацию, сведения или данные, но не электронные документы. В этой связи использование сложных и дорогостоящих электронных сервисов доверия ПД-Т может оказаться экономически и организационно нецелесообразным.

Предполагается, что различные информационно-аналитические системы в совокупности с системами маркировки товаров, предназначенные в том числе для мониторинга товарных потоков конечным потребителем, могут использовать информационные ресурсы из учетных и информационно-справочных систем в соответствии с заранее заданным аналитическим алгоритмом для контрольных целей и пресечения возможных правонарушений.

Вопросы обеспечения защиты коммерческой тайны и персональных данных, а также юридической значимости электронных документов могут основываться на следующих общих архитектурных принципах:

- скоординированная организация, специализированная международная нейтральная сеть уполномоченных операторов, по аналогии с Trusted Third Party (ТТР) или Accountability Agents (АА);
- определение для таких операторов организационных, технологических, правовых и институциональных требований;
- определение требований по проведению независимого аудита таких операторов;
- проведение независимого комиссионного аудита операторов согласно установленным требованиям;
- регламентация доступа с клиентского уровня к нужным сведениям (коммерческая тайна, персональные данные, электронные документы), за которые несут регламентированную ответственность уполномоченные операторы.

Для учетных систем целесообразно выделить два уровня: корпоративный и общего пользования. При этом могут использоваться различные транспортные решения:

- набор информационных шин, шлюзов, систем межведомственного электронного взаимодействия, а также выделенные каналы связи – для корпоративных систем;
- сеть Интернет и аналоги – для систем общего пользования.

Для целей эффективного программного управления формированием ЕЦП целесообразно разграничивать сегменты – интеграционный и национальные – по критерию централизации или децентрализации деятельности уполномоченных функциональных или инфраструктурных операторов.

Национальные сегменты ЕЦП целесообразно организационно и финансово разграничивать с архитектурными элементами национальных электронных правительств, при их тесном общесистемном взаимодействии.

Национальные системы единого окна должны опираться на технологические инфраструктуры национальных сегментов ЕЦП и электронных правительств и при этом нацеливаться, в основном, на оптимизацию административных и бизнес процессов (реинжиниринг) в сквозном режиме между всеми категориями субъектов электронного взаимодействия в различных странах и уровнями управления, например, наднациональный, государственный, региональный и муниципальный.

### **Построение трансграничного пространства доверия на централизованных или децентрализованных принципах**

Для целей поддержки ЕЦП трансграничное пространство доверия может сегментироваться по признаку централизованного или децентрализованного управления сервисами доверия.

**Централизованная модель построения инфраструктуры доверия.** Определенное развитие на протяжении ряда последних лет получила централизованная модель, в разработке которой принимали участие авторы настоящей статьи. Ее можно обозначить как нейтральную международную среду для отдельных стран и их объединений, устойчивую по отношению к политическим, экономическим, социальным и иным влияниям и интересам отдельно взятых ее участников.

Доверие, являясь само по себе фундаментально общественной функцией, строится в централизованной модели на общественных отношениях, институционализированных самими же участниками соответствующей инфраструктуры доверия. Централизованная модель основывается на выполнении всеми ее участниками между ними же согласованных Требований при проведении периодического независимого аудита уполномоченных операторов сервисов доверия.

Таким образом, необходимый уровень доверия между участниками (в том числе – конечными пользователями) инфраструктуры доверия, основанной на централизованной модели, достигается благодаря априорно институционализированным отношениям между странами – участницами этой инфраструктуры доверия. Эта институционализация охватывает юридические и организационные аспекты, влияющие и на технико-технологические аспекты интероперабельности и информационной безопасности.

Существенными особенностями централизованной модели доверия являются:

- ее естественное и поэтому легкое сопряжение с традиционно существующими институтами (включая идентификацию субъектов электронного взаимодействия);
- государственно-коммерческое сотрудничество в рамках инфраструктуры доверия;
- ее естественная масштабируемость (прием новых участников / выход из инфраструктуры доверия);
- равноправность и недискриминационность сотрудничества в инфраструктуре доверия;
- многовариантность выбора уровня квалификации отдельных сервисов доверия (например, низкий, средний, высокий).

Подходы к построению нейтральной среды находят отражение в ряде международных документов, среди которых следующие:

- Договор о Евразийском экономическом союзе (подписан в г. Астане 29.05.2014)<sup>1</sup>;
- Проект рекомендации Центра ООН по упрощению торговых процедур (СЕФАКТ) «Об обеспечении юридически значимого трансграничного электронного взаимодействия»<sup>2</sup>;
- Проект регионального межправительственного соглашения об упрощении процедур трансграничной безбумажной торговли Экономической и социальной комиссии ООН стран Азии и Тихого океана (ЭСКАТО)<sup>3</sup>;
- пакет документов в области формирования и функционирования трансграничного пространства доверия государств-участников СНГ<sup>4</sup>.

Практическая реализация нейтральной международной среды на платформе доверенной третьей стороны в настоящее время активно проводится в рамках Евразийской экономической комиссии. Разработан проект архитектуры трансграничного пространства доверия, который включает набор централизованно предоставляемых электронных сервисов. Продолжается обсуждение государствами-членами ЕАЭС их состава в контексте согласованного обеспечения вопросов международной и национальной информационной безопасности.

**Децентрализованная модель построения инфраструктуры доверия.** Необходимый уровень доверия может также обеспечиваться инфраструктурами доверия, построенными по децентрализованной модели.

---

<sup>1</sup> URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_163855/](http://www.consultant.ru/document/cons_doc_LAW_163855/)

<sup>2</sup> URL: <http://www1.unecp.org/cefact/platform/download/attachments/55378391/Rec+draft+v.0.91+08.09.15.pdf>

<sup>3</sup> URL: <http://www.unescap.org/our-work>

<sup>4</sup> URL: <http://www.rcc.org.ru/work/informatiz/trans/index>



Одной из технологий, позволяющей реализовать децентрализованную модель, является *блокчейн (blockchain)*. Идея блокчейн-технологии максимально проста: это огромная база данных общего пользования, которая функционирует без централизованного руководства. В случае с биткоином проверкой транзакций занимаются так называемые майнеры — участники системы, которые подтверждают подлинность совершенных действий, а затем формируют из записей транзакций блоки. В настоящее время в обществе развернуты активные дискуссии по вопросу перспективности использования блокчейн-технологии в массовых сервисах<sup>1</sup>.

Доверие, являясь само по себе фундаментально общественной функцией, строится в децентрализованной модели на общественных отношениях, возникающих между участниками децентрализованной инфраструктуры доверия, основанных на неконтролируемости решающего большинства узлов блокчейн-системы<sup>2</sup> и их равноправности.

Таким образом, мы видим, что децентрализованная модель установления доверия также требует институционализации, несмотря на то, что неконтролируемость решающего большинства узлов блокчейн-системы и их равноправность в значительной мере поддерживается (но не обеспечивается полностью) математическими / технологическими, а не организационными (как в централизованной модели) методами.

Поскольку сам процесс майнинга сопряжен со сложными математическими задачами, майнеры должны иметь в своем арсенале довольно мощные компьютеры. В руках этих участников и находится распределенная база данных, состоящая из «цепочки блоков». Распределенный характер базы данных на основе блокчейна и позволяет контролировать достоверность транзакций без надзора каких-либо институционализированных (например, финансовых) регуляторов.

Основное преимущество блокчейна перед традиционными транзакциями — отсутствие посредников (например, в лице банков). Сейчас все операции с деньгами, документами или другими данными неизбежно проходят через посредников. Банки, государственные органы или же нотариусы постоянно подтверждают подлинность проделанных операций.

Блокчейн не имеет центрального органа, поэтому транзакции проверяются всеми участниками системы. Именно это позволяет избавиться от посредников и тем самым упростить процедуру. Программный код сети открыт, и любой может обратиться к нему, но личность и другая персональная информация остаются тайной. Все, что видят создатели блоков, — данные по каждой конкретной операции.

---

<sup>1</sup> URL: <http://www.gazeta.ru/tech/2016/02/01/8038769/blockchain.shtml>

<sup>2</sup> „Blockchain“-система: какая-либо конкретная реализация „blockchain“-технологии.— *Авт.*

Проще говоря, если блокчейн-технология внедрить в повседневную жизнь, то контроль по фиксации операций со стороны банков, госорганов, аудиторов, контролеров, страховых компаний или регистраторов будет либо нужен в существенно меньшем объеме, либо вовсе не нужен.

В будущем государства могут институционализировать определенные блокчейн-системы и взять на вооружение данные, заверенные с помощью институционализированного блокчейна, как доказательства в различных процессах, в том числе и судебной практике, поскольку технология не принимает какую-либо фальсификацию. Российские специалисты занимаются разработкой шлюза для взаимодействия с биткоин-блокчейн для нотариализации событий.

Блокчейн-технология представляет собой новое, перспективное явление современных информационно-коммуникационных технологий, вызывает множество дискуссий в части возможных сопутствующих негативных проявлений, особенно при использовании цифровой валюты bitcoin, поэтому на этом аспекте ниже будет сосредоточено основное внимание.

**Основные свойства блокчейн-технологии.** Blockchain – это специфическая информационная технология (ИТ), обеспечивающая практически неподдельваемое сохранение полной истории завершенных транзакций переприсвоения набора атрибутов от одного адреса блокчейн-системы к другому. Незавершенные, то есть непринятые, блокчейн-системой транзакции системой не регистрируются и, следовательно, в ней не существуют. Завершенная транзакция не может быть отозвана.

Полнота истории всех транзакций внутри данной блокчейн-системы является имманентным свойством этой ИТ и обеспечивается соответствующей процедурой построения цепочки отдельных блоков (учетных записей).

Практическая неподдельваемость истории, то есть протокола завершенных транзакций, обеспечивается множественной репликацией протокола транзакций на децентрализованно организованной сети равноправных (peer-to-peer) узлов системы.

Множество узлов системы должно быть настолько мощным, чтобы оно не могло контролироваться одним оператором или картелем операторов. Неконтролируемость решающего большинства узлов системы и их равноправность являются основой установления необходимого уровня доверия между участниками системы.

Полнота и неподдельваемость истории всех завершенных транзакций внутри данной блокчейн-системы являются сервисами доверия, предоставляемыми системой посредством блокчейн-технологии. Проведение транзакций и сохранение их истории являются функциональным сервисом блокчейн-системы.

Следует отметить, что имманентная блокчейн-системе полнота протокола всех завершенных транзакций приводит к имманентной немасштабируемости одной и той же системы. Если требование масштабируемости должно быть выполнено, то это с необходимостью приведет к эксплуатации многих независимых блокчейн-систем. Побочным эффектом немасштабируемости может стать либо понижение функциональной производительности системы, либо необходимость постоянного увеличения системных ресурсов (мощности).

Транзакция в рамках блокчейн-системы состоит в том, что определенная совокупность атрибутов, приписанных адресу А, переприсваивается (перемещается) адресу Б в рамках системы. Соответствующая учетная запись о транзакции содержит (i) – отсылку-линк к предыдущей транзакции, (ii) – штамп времени актуальной транзакции, (iii) – hash транзакции (переприсвоение атрибута Т от адреса А адресу Б) и (iv) – nonce (number used once – одноразовый номер, вычисляемый методом проб и ошибок).

Протокол транзакций как таковых доступен всем, то есть конфиденциальность транзакций вынесена за скобки блокчейн-технологии.

Что может служить атрибутом в рамках этой технологии? Теоретически здесь нет специальных ограничений. Это могут быть атрибуты собственности и владения (но не *права* собственности или владения, пока система не институционализована), любые другие статусы (но не правовые, пока система не институционализована), атрибуты какого-либо объекта, например, драгоценного камня или другого товара (услуги).

В силу принципиальной равноправности узлов системы блокчейн-технология оставляет за скобками создание (первичное присвоение) атрибутов отдельным адресам системы. Если система должна обрабатывать, кроме прочего, юридически значимые атрибуты, то институциональная интеграция этой системы совершенно неизбежна.

Блокчейн-технология использует неподделяемые адреса участников блокчейн-системы. Их конкретная спецификация должна быть неотъемлемой частью системы. Например, в системе bitcoin адреса с таким свойством реализованы на базе асимметричной криптографии (открытых и закрытых ключей).

Блокчейн-технология полностью оставляет за скобками привязку системного адреса к физическим и юридическим лицам. Если система должна обрабатывать, кроме прочего, атрибуты, институционально присвоенные физическому или юридическому лицу (например, определенная квалификация – врач), то ее институциональная интеграция, включая использование систем идентификации, совершенно неизбежна.

**Использование блокчейн-технологии.** Характер данных, обрабатываемых блокчейн-технологией, – это протоколы транзакций. Поэтому эта технология наиболее просто применима к документам, представляющим

собой протоколы переприсвоения (перехода) атрибутов от одной инстанции к другой.

В этом контексте мы задаемся вопросом: атрибуты какого типа наиболее естественно и адекватно могут обрабатываться блокчейн-технологией?

Это атрибуты, относительно часто меняющие свою «прописку», например, атрибут собственности или атрибут владения, атрибут ответственности и т. п. Участники транзакции обычно желают документирования изменения «прописки» атрибута.

Одним из широко распространенных видов документов с таким признаком являются оборотные документы и ценные бумаги: транспортные накладные, коносаменты, сертификаты происхождения (например, драгоценных камней, автомобилей, другой ценной движимости), записи о владении недвижимостью, облигации, чеки на предъявителя. Денежные знаки также относятся к оборотным документам.

С договором (а не фактом) купли-продажи недвижимости, например, будет уже сложнее: для описания предмета договора необходимо большое количество не вполне стандартизированных атрибутов, полностью описывающих предмет договора и частично меняющихся в зависимости от конкретного предмета договора (специфические параметры и особенности недвижимости).

Такие наборы не вполне стандартизированных атрибутов не совсем укладываются в парадигму блокчейн-технологии, которая наиболее эффективна при обработке протоколов стандартизированных транзакций, и поэтому потребуют дополнительных усилий по реализации в рамках блокчейн-системы.

Полнота и неподделываемость протокола являются имманентными сервисами доверия, реализуемыми блокчейн-технологией. Давайте представим себе решение, при котором неподделываемые адреса блокчейн-системы однозначно привязаны к личностям стоящих за ними физических и юридических лиц, и эта привязка разрешима, то есть адреса не анонимны. Тогда вся история транзакций для любого субъекта права, участвующего в системе, будет доступна всем. Это бы повлекло за собой драматическое усечение личной сферы пользователей системы и противоречило бы современному пониманию защиты персональных данных.

Таким образом, если защита персональных данных останется в фокусе внимания общества, то блокчейн-системы, удовлетворяющие условиям этой защиты, должны быть:

- либо анонимны: самое естественное приложение – анонимные ценные бумаги, включая деньги, сертификаты происхождения ценных активов (драгоценностей, произведений искусства, дорогих автомобилей и т. п.) и другие анонимные оборотные средства;

- либо дополнены свойством конфиденциальности и ограничения доступа к персональным данным;
- либо использоваться замкнутым и ограниченным кругом пользователей, которые все доверяют оператору системы (такая реализация, правда, нарушит принцип доверия в блокчейн-системах: необходимый уровень доверия между участниками системы основывается на неконтролируемости решающего большинства узлов системы и их равноправности, а не на организационном доверии какой-то специальной роли).

**Влияние на общество.** Следует заметить, что правовая база любой юрисдикции в прошлом, настоящем и будущем основывается на идентификации физических и юридических лиц. Это является имманентным, неотторжимым свойством права как социально организующей функции человеческого общества, так как пользователями правовой системы являются именно физические и юридические лица — как подмножество ее субъектов. Сбор налогов для поддержания функционирования общества как такового и сохранение баланса между защитой общества от угроз и свободой выбора для его членов также основываются на идентификации физических и юридических лиц.

Широкое внедрение блокчейн-систем в различные сферы общественной жизни может существенно повлиять как на инфраструктурную организацию общества, так и на процедуры его регулирования. Если блокчейн-системы будут институционально интегрированы и, следовательно, результаты их действия будут признаваться в качестве доказательств в правосудии, это приведет, например, к уменьшению объема функций исполнительной власти из-за перенятия блокчейн-системами некоторых, а то и многих ее институциональных функций.

Например, одна из центральных функций государства — фиксация отношений собственности между физическим или юридическим лицом и каким-либо активом (asset) — может быть перенята блокчейн-системами. Обеспечение соблюдения отношений собственности останется, однако, — в ведении правосудия.

Сокращение объема функций исполнительной власти автоматически приведет к уменьшению ее представительского авторитета. Этот процесс, как любое существенное изменение структур и функций в этой сфере, может сопровождаться политической нестабильностью.

Кроме того, возможным в перспективе представляется появление следующих факторов:

- уменьшение роли нотариата, особенно в области подтверждения юридически значимых статусов субъектов и объектов права, так как фиксация этих статусов может быть перенята блокчейн-системами.

Правовая оценка юридически значимых статусов останется в ведении правосудия;

- драматическое уменьшение роли поставщиков (предоставителей) финансовых услуг, особенно тех, которые в основном занимаются посредничеством при проведении платежной транзакции между покупателем и продавцом (это в особенности коснется банков и платежных площадок в интернете);
- изменение конкурентной ситуации в международной экономике в пользу развивающихся стран. Фиксация собственности блокчейн-системами (например, на землю, другую движимость и недвижимость) способствовало бы появлению в этих странах кредитоспособных хозяйственных субъектов (собственников), что, в свою очередь, привело бы к ростовому скачку их экономик.

Следует обратить внимание еще на одно явление, которое имманентно блокчейн-технологии, по крайней мере в ее сегодняшнем виде. Для создания новых значимых (то есть валидных) блоков в блокчейн-системе используются методы Proof-of-Work и Proof-of-Stake.

Метод Proof-of-Work требует тем меньше вычислительных ресурсов (экспоненциально), чем раньше участник системы к ней присоединился. Таким образом, ранние участники системы получают существенные ресурсные преимущества, что несколько противоречит заявленному равноправию участников. Для поддержания принципа равноправия конкретные блокчейн-системы, использующие Proof-of-Work, могут вводить как дополнительные технические, так и технико-организационные средства. Например, в системе bitcoin к ним относятся *targeting*, регулирующий с помощью специального системного параметра трудность создания новых значимых (т. е. валидных) блоков, и мотивация майнеров<sup>1</sup> (получением bitcoins) для увеличения количества независимых пользователей системы.

Метод Proof-of-Stake мотивирует к накоплению контролирующих атрибутов системы в одних руках с целью перенятия контроля над системой, что противоречит принципу децентрализации системы.

Любая из этих реализаций – без введения дополнительных технических и организационных мер противодействия – с необходимостью приведет к возникновению олигархической системы, в которой небольшая группа ее участников сможет (и будет) контролировать поведение системы. Уровень доверия к этой системе будет зависеть от уровня доверия к тому, что группа олигархов не злоупотребляет своим положением в системе. Это противоречит изначально заявленным принципам неконтролируемости решающего большинства узлов системы и их равноправности. Более того, плакатное

---

<sup>1</sup> Участники системы, подтверждающие подлинность совершенных транзакций, а затем формирующие из записей транзакций блоки.

декларирование этих принципов вуалирует имманентную склонность сегодняшних реализаций блокчейн-технологии к образованию форм олигархии.

Предложенная в проекте рекомендации Центра ООН по упрощению торговых процедур (СЕФАКТ) «Об обеспечении юридически значимого трансграничного электронного взаимодействия»<sup>1</sup> нейтральная международная среда, контролируемая клубом юрисдикций на равноправных началах, а не одним государством, является, на наш взгляд, более универсальной в отношении приложения в различных областях человеческого общества. В отношении установления доверия она соединяет преимущества относительного равноправия блокчейна как децентрализованной технологии и преимущества относительно легкой институциональной интегрируемости и легкой масштабируемости централизованных систем.

Централизованная система, построенная на нейтральной среде, кроме прочего, легко взаимодействует с системами идентификации лиц (и может их легко интегрировать при необходимости) и, таким образом, может гибко регулировать баланс «идентификация – анонимность».

Блокчейн-технология наряду с другими технологиями может эффективно использоваться для реализации частных задач, для решения которых она предоставляет адекватную среду. Как было обосновано выше, самое естественное приложение блокчейн-технологии – анонимные ценные бумаги, включая деньги, сертификаты происхождения ценных активов (драгоценностей, произведений искусства, дорогих автомобилей и т. п.) и другие анонимные оборотные средства.

### **Сравнительный анализ централизованной и децентрализованной моделей построения трансграничного пространства доверия**

**Общие замечания.** Разрабатывая архитектуру цифровой экономики, необходимо стремиться описать ее максимально полно, непротиворечиво и выявить ключевые аспекты сходства и различий между основными элементами, прежде всего по одному из ключевых вопросов – способам обеспечения доверия в сетях массового пользования.

Очевидно, что блокчейны стали явлением современных информационно-коммуникационных технологий, что можно игнорировать в контексте международного правового регулирования, учитывая множество известных угроз, с этим связанных, но полезнее выявить принципиальную разницу на архитектурном уровне с тем, чтобы найти место всем подходящим способам

---

<sup>1</sup> URL: [http://www1.unece.org/cefact/platform/download/attachments/55378391/Rec + draft + v.0.91 + 08.09.15.pdf](http://www1.unece.org/cefact/platform/download/attachments/55378391/Rec+draft+v.0.91+08.09.15.pdf)

обеспечения доверия, которое является само по себе фундаментально общественной функцией.

Как уже было указано выше, ПД-Т может сегментироваться по признаку *централизованного* или *децентрализованного* управления сервисами доверия.

*Централизованная* модель разрабатывается в настоящее время в ряде международных форматов. В ней доверие строится на общественных отношениях, институционализированных самими же участниками соответствующей инфраструктуры доверия. Централизованная модель основывается на выполнении всеми ее участниками между ними же согласованных Требований при проведении периодического независимого аудита уполномоченных операторов сервисов доверия. Таким образом, необходимый уровень доверия между участниками (в том числе – конечными пользователями) инфраструктуры доверия, основанной на централизованной модели, достигается благодаря априорно институционализированным отношениям между странами – участниками этой инфраструктуры доверия. Эта институционализация охватывает юридические и организационные аспекты, влияющие и на технико-технологические аспекты интероперабельности и информационной безопасности.

Блокчейны как технология позволяют построить *децентрализованную* модель управления сервисами доверия. В ней доверие строится на общественных отношениях, возникающих между участниками децентрализованной инфраструктуры доверия, основанных на неконтролируемости решающего большинства узлов блокчейн-системы одной инстанцией и на их равноправности. Таким образом, становится очевидным, что децентрализованная модель установления доверия также требует институционализации, несмотря на то, что неконтролируемость решающего большинства узлов блокчейн-системы и их равноправность в значительной мере поддерживается (но не обеспечивается полностью) математическими / технологическими, а не организационными – как в централизованной модели – методами.

Законодательство, государственное управление, право, экономика и многие другие области человеческого общества исторически основываются на парадигме централизованной модели.

Современное законодательство регулирует и те сферы, где в перспективе возможно внедрение блокчейн-технологии, но при этом оно ориентировано на принцип «централизованного реестра». Соответственно, для того, чтобы сделать возможным применение технологии «распределенного реестра», необходимо будет изменить соответствующие части законодательства, как национального, так и международного.

Это видение в терминах централизованного и распределенного реестра хорошо раскрывает суть различий.



Для нейтральной международной среды принцип «централизованного реестра» – это совокупность учетных систем, поддерживаемых трансграничным или национальным пространством доверия, а ведение централизованного реестра должно быть возложено на специально уполномоченного доверенного оператора. Доверие строится здесь на общественных отношениях, институционализированных самими же участниками соответствующей инфраструктуры доверия.

Распределенный реестр – это глобальный вычислительный комплекс, функционирующий по сложному и при этом надежному алгоритму. Доверие строится здесь на общественных отношениях, возникающих между участниками децентрализованной инфраструктуры доверия, основанных на неконтролируемости решающего большинства узлов блокчейн-системы одной инстанцией и на их равноправности.

**Описание различий между централизованной и децентрализованной моделями.** Одним из центральных различий между обеими моделями является их отношение к идентификации и анонимности субъектов взаимодействия.

Любая существующая правовая система опирается на однозначную идентификацию субъектов взаимодействия (физических, юридических и уполномоченных лиц). Например, анонимные заявления не имеют юридической силы.

Ключевой имманентной особенностью при использовании децентрализованной модели, основанной на блокчейн-технологии, является анонимность участников информационного взаимодействия. Очевидно, что в прикладных системах можно дополнить блокчейн-технологии идентификацией участников, например, биометрической, но это не является имманентным самой блокчейн-технологии. Следует также отметить, что в случае потери анонимности в рамках блокчейн-технологии вся история транзакций для любого субъекта права, участвующего в системе, может быть общедоступной.

Для реализации нейтральной международной среды в рамках централизованной модели вводится специальный посредник между субъектами – доверенная третья сторона, которая должна иметь специализированную институциональность. Институты всегда опираются на деятельность особых категорий доверенных лиц, например, таможенников или нотариусов. В самом общем случае некоторое уполномоченное лицо, являясь субъектом прав, обеспечивает легитимность информационного взаимодействия любых других лиц – тоже субъектов прав, в том числе в трансграничном режиме. В силу анонимности участников блокчейн-систем в рамках децентрализованной модели принципиально невозможно ввести какой-либо институт уполномоченных лиц. Соответственно, децентрализованная модель, основанная на блокчейн-системах, доверенно фиксирует не субъекты взаимодействия, а полную

историю завершенных транзакций между ними, в то время как централизованная модель с нейтральной средой отвечает за весь комплекс взаимодействия, включая легитимность самой доверенной третьей стороны.

Опираясь на указанные выше существенные особенности централизованной модели доверия (см. выше о «централизованной модели построения инфраструктуры доверия»), мы далее обратим внимание на дальнейшие важные различия между обеими моделями:

- централизованная модель естественно и поэтому легко сопрягается с традиционно существующими институтами (включая идентификацию субъектов электронного взаимодействия). Децентрализованная вступает в противоречие с существующими институтами;
- централизованная модель естественно поддается правовому регулированию, как национальному, так и международному. Основные сложности для правового регулирования децентрализованной модели возникают в связи с категорией анонимов<sup>1</sup> и имманентной децентрализованностью — и, следовательно, неконтролируемостью — ее инфраструктуры;
- централизованная модель позволяет непротиворечиво организовать государственно-частное партнерство в рамках инфраструктуры доверия. Для децентрализованной модели контроль и аудит являются «инородными телами»;
- централизованная модель обладает естественной масштабируемостью в рамках приема новых участников или выхода из инфраструктуры доверия. В децентрализованной модели, основанной на блокчейн-технологии, масштабируемость может достигаться только созданием новых, независимых друг от друга блокчейн-систем;
- централизованная модель предполагает равноправное и недискриминационное сотрудничество в рамках общей инфраструктуры доверия. Децентрализованная модель без дополнительного регулирования обладает склонностью к образованию олигархий в своих пределах;
- централизованная модель предоставляет многовариантность выбора уровня квалификации отдельных сервисов доверия (например, низкий, средний, высокий). Децентрализованная модель имеет полярный «черно-белый» характер: транзакция состоялась: да — нет;
- централизованная модель имманентно концентрирует ресурсы у доверенной третьей стороны. Децентрализованная модель предполагает существенную распределенность инфраструктуры и ее ресурсов.

---

<sup>1</sup> Не ясно отнесение категории анонимов к объектам или субъектам прав: с одной стороны, они обладают волеизъявлением, участвуя в цепочках транзакций; с другой — они сами являются объектами автоматизированного учета.

**Вопросы конвергенции.** На наш взгляд, неверно утверждать, что одна из рассмотренных выше моделей в любом случае подходящая, а другая заведомо влечет негативные проявления. Логика развития общества приводит к существованию исторических фаз с различным уровнем взаимного доверия между его отдельными членами, группами и общественными институтами. Фактическое или ощущаемое отсутствие необходимой степени взаимного доверия и другие мотивации делают неизбежной незаконную деятельность при использовании конкретной технологии, что и вызывает регулятивное вмешательство со стороны общества.

Оптимальной стратегией того, что касается предотвращения негативных последствий использования цифровых валют, могло бы стать появление общественно приемлемых альтернатив тому, что стимулирует их принятие, а это прежде всего – анонимность транзакций, безопасность (полнота и неподдельность истории всех завершенных транзакций) и доступность, которые интересны массовым пользователям.

В приемлемости со стороны общества на данном историческом этапе и заключаются предпосылки для конвергенции между двумя подходами.

Сложные человеко-машинные системы неизбежно будут эволюционировать в сторону усиления машинной компоненты. При этом представляется важным, как и в медицине, – не навредить.

Поэтому рассматривая вопрос построения трансграничного пространства доверия – неадекватно исходить из преимущественно технологической парадигмы, например, предлагая механическую комбинацию блокчейн-технологии с какими-либо сервисами доверия.

Как уже отмечалось, основная институциональная проблема децентрализованной модели, построенной на блокчейн-технологии, заключается в том, что невозможно локализовать информационные системы – распределенные реестры и закрепить за ними уполномоченных операторов, которые могут подлежать международному правовому регулированию. С другой стороны, централизованные реестры – учетные системы – допускают естественное и поэтому легкое сопряжение с традиционно существующими институтами. Соответственно можно построить правовую модель и предложить ее международному сообществу для регулирования, что и происходит в рамках СЕФАКТ, ЭСКАТО, ЕАЭС и СНГ, как описано выше.

В качестве промежуточного вывода можно отметить, что нейтральная международная среда, контролируемая клубом юрисдикций на равноправных началах, а не одним государством, является, на наш взгляд, в обозримой перспективе более универсальной в отношении приложения в различных областях человеческого общества. В отношении установления доверия она соединяет преимущества относительного равноправия блокчейна – как децентрализованной технологии – и преимущества относительно легкой

институциональной интегрируемости и легкой масштабируемости централизованных систем.

Однако это не означает, что децентрализованные решения нужно запретить или отпустить «в свободное плавание». Как мы уже отмечали, децентрализованная модель установления доверия также требует институционализации, несмотря на то, что неконтролируемость решающего большинства узлов блокчейн-системы и их равноправность в значительной мере поддерживается (но не обеспечивается полностью) математическими / технологическими, а не организационными – как в централизованной модели – методами. По блокчейн-технологии, однако, пока в мире не предложена модель правового регулирования, что является определенным барьером на пути развития глобального информационного общества, и на этот вызов надо отвечать.

Пока не очень понятно, как использовать блокчейн-технологии в рамках, например, электронного правительства в ближайшей обозримой перспективе, без радикальной смены парадигмы взаимодействия власти и общества. С другой стороны, эту технологию можно и нужно легализовать в тех сферах, где она может эффективно использоваться для реализации частных задач, для решения которых она предоставляет адекватную среду. Как указывалось выше (см. «Децентрализованная модель построения инфраструктуры доверия»), самое естественное приложение блокчейн-технологии – анонимные ценные бумаги, включая деньги, сертификаты происхождения ценных активов и другие анонимные оборотные средства. Другой сферой ее возможного применения может быть, например, урегулирование споров в режиме онлайн.

Оптимальным решением является конвергенция и выработка непротиворечивых моделей международного правового регулирования, нацеленных на достижение общественного блага, использование разносторонних преимуществ и недопущение негативных проявлений.

**Вопросы реализации.** Практическую реализацию двухсегментного трансграничного пространства доверия невозможно проводить без тесной увязки с функциональными сервисами, то есть эту проблему надо рассматривать в общем контексте цифровой экономики. Результатом могут стать две различные правовые модели для централизованного-децентрализованного учета, которые также требуют более широкого концепта прикладных сервисов.

Правовому регулированию подлежат объекты и субъекты прав. К субъектам можно отнести все категории лиц (физические, юридические, уполномоченные) и организации (органы власти всех уровней, судебные, страховые и нотариальные инстанции), а также операторов информационных систем. К объектам – информационные системы и рабочие места, включая средства подписи и доступа. Между субъектами и объектами прав возникают правовые отношения – в первую очередь по поводу функциональных приложений.

Эти правовые отношения, однако, могут также включать аспекты доверия и безопасности, что может рассматриваться как опция к торговле, медицине и образованию. Само по себе доверие бессмысленно – оно всегда относится к кому-то или чему-то. Именно поэтому блокчейн-технология появилась в связке с цифровой валютой – биткоинами. Как известно, технологии сами по себе не подлежат правовому регулированию, а являются сферой специфического технического регулирования, которое находится вне компетенции таких субъектов регулирования, как Комиссия ООН по праву международной торговли (ЮНСИТРАЛ), в ведении которой находится проблематика институционализации двухсегментного трансграничного пространства доверия.

Подводя итог, можно предложить инициативу по разработке проекта Конвенции ООН об использовании трансграничного пространства доверия для цифровой экономики. Такого рода вклад может быть сделан в профильную Рабочую группу IV (Электронная коммерция) ЮНСИТРАЛ.

При этом в качестве возможного решения проблемы двух правовых моделей доверия можно предложить следующий подход: нейтральная международная среда, контролируемая клубом юрисдикций на равноправных началах, и ее общая инфраструктура доверия строятся на принципе международного регулирования, в то время как сервисы на основе блокчейн-технологии предоставляются на основе саморегулирования при дозированном международном контроле с целью недопущения нежелательных для общества эффектов. Таким образом, ключевым вызовом в отношении реализации централизованной модели станет поиск консенсуса по регламенту организации нейтральной международной среды, тогда как ключевым вызовом в отношении реализации децентрализованной модели станет поиск приемлемых форм такого регулятивного вмешательства, которое не станет существенным препятствием для применения блокчейн-технологии.

## **Выводы**

Предложенные базовые архитектурные – централизованный и децентрализованный – подходы могут оказать существенную помощь для последующей выработки в специализированных структурах ООН и профильных международных организациях семейства рекомендаций в области формирования и функционирования ЕЦП, а также при подготовке различных концепций, стратегий и других основополагающих документов в интеграционных объединениях, планы которых предусматривают построение ЕЦП. Очевидно, что при построении конкретных информационных систем в рамках ЕЦП будет взаимопроникновение между отдельными элементами описанных базовых архитектур.

СБОРНИКИ ПРЕЗИДЕНТСКОЙ БИБЛИОТЕКИ

СЕРИЯ

**ЭЛЕКТРОННОЕ  
ЗАКОНОДАТЕЛЬСТВО** §

Выпуск 6

В сборнике опубликованы материалы международной научно-практической конференции «Право и информация: вопросы теории и практики», проведенной 15 апреля 2016 г. ФГБУ «Президентская библиотека имени Б. Н. Ельцина».

Материалы, представленные в выпуске, сгруппированы в два раздела. Специальный раздел посвящен перспективным направлениям совершенствования законодательства, прежде всего – интеллектуальным правам в сфере доступа к информации в библиотеках. Во втором разделе собраны материалы по информационному праву. В частности, освещаются вопросы регулирования обращения с персональными данными, деятельности СМИ, а также правовой информатики.

В приложении к сборнику представлены материалы виртуальной выставки «Из истории развития российского законодательства о печати».