Информационно-правовые основы правоприменения в цифровой сфере

Ловцов Д. А.[*]

Ключевые слова: *информационное право, информационная сфера (инфосфера), информационно-цифровая сфера, информационные правоотношения, информационно-цифровое пространство, цифровое пространство, цифровые права, цифровые технологии, блокчейн, информационная безопасность, правоприменение, концептуально-логическая модель.*

Аннотация.

Цель работы: совершенствование научно-методической базы правоприменения в информационно-цифровой сфере общественно-производственной деятельности.

Метод: системный анализ информационных правоотношений, цифровых технологий (включая блокчейн) и цифровых прав; концептуально-логическое моделирование информационно-цифровой сферы.

Результаты: определены специфические объекты информационных правоотношений в инфосфере; рассмотрены система, актуальные цифровые объекты и специальные методы современного информационного права; обоснована продуктивная классификация цифровых технологий; исследованы состояние правовой регламентации «цифровых прав» в России и уровень информационной безопасности блокчейн-технологии; определены состояние и пути решения проблем цифровой трансформации инфосферы с целью обеспечения эффективности мониторинга правоприменения в цифровой сфере; уточнена концептуально-логическая модель инфосферы с учетом цифровой трансформации.

Обоснованы выводы: об объективности тенденции концептуального перехода в отечественном правоведении к системно-математическим представлениям о праве; о невозможности развития цифровой экономики в России без легализации криптовалюты в гражданском законодательстве; о неочевидности информационной безопасности блокчейн-технологии; о необходимости межведомственного развития единого информационно-цифрового пространства и коллективной разработки нормативного организационно-правового обеспечения совместного функционирования ведомственных информационных систем, участвующих в процессе правоприменения.

DOI: 10.21681/2226-0692-2020-2-44-52

Введение

Правовое регулирование различных *информационных отношений*, возникающих в информационной сфере (инфосфере) общественно-производственной (правоохранительной и др.) деятельности, представляющих собой одновременно и средство для достижения конкретных целей, и определенный результат именно *информационной* деятельности, т. е. *целевых*[1] информационных отношений [8], реализуется на основе применения норм относительно новой интегрированной (частично самостоятельной и частично комплексной) отрасли *информационного права* [1, 7, 19, 20].

Объектами целевых информационных правоотношений (*информационных правоотношений в инфосфере*) являются компоненты информационной деятельности. *Информационная деятельность* — это деятельность в инфосфере как форма целесообразного преобразования (изменения) информационного содержания окружающего материального и духовного мира в интересах людей, общества или государства, включающая:

- *цель* (материальные или духовные блага, в том числе информационные продукты и услуги, продукты интеллектуального творчества и др.);
- *информационные средства* (устройства, комплексы, системы; коммуникации, технологии);
- *информационные ресурсы* (совокупность запасов *содержательной*[2] информации — информационно-со-

[1] Например, отношения, возникающие при производстве и распространении массовой информации, при применении процедур обеспечения информационной безопасности, при создании и функционировании Государственных автоматизированных систем РФ «Выборы», «Правосудие», «Управление», при создании и функционировании глобальных телематических сетей и др. В отличие от *обеспечивающих* информационных отношений, являющихся объектом правового регулирования иных отраслей права.

[2] Например, массовой информации, судебной, оперативно-розыскной, конъюнктурно-экономической, патентно-лицензионной, конструкторской, сведений о ноу-хау, персональных данных, сведений о факте усыновления, инсайдерской информации на рынке ценных бумаг и др.

[*] ***Ловцов Дмитрий Анатольевич,*** доктор технических наук, профессор, заслуженный деятель науки Российской Федерации, заведующий кафедрой информационного права, информатики и математики Российского государственного университета правосудия, г. Москва, Российская Федерация. E-mail: dal-1206@mail.ru

держательный ресурс и возможностей *структурной*[3] информации — информационно-структурный ресурс эргасистем);

- *информационные структуры* (информационные массивы и операции преобразования содержательной информации);
- *информационные процессы* (производство, интерпретация, коммуникация информации, отражающие поведение, действия и интересы информационных деятелей);
- *информационно-правовые режимы* (комплексы средств правового регулирования информационных отношений, возникающих при установлении и применении разнокачественных форм существования и представления информации);
- *организационные и юридические структуры* (определяют фактическое содержание информационного правоотношения, имеют частные или государственные интересы);
- *результаты* (информационные продукты, услуги; интеллектуальная собственность; информационные отношения, определяющие, в частности, фактическое создание, преобразование, передачу, получение, логическую обработку, интерпретацию, предоставление, использование, неразглашение информации и др.).

Базовыми структурными компонентами при этом являются *информационные средства* и *информационные ресурсы* («дополнительные» средства).

Научно-технический уровень информационных средств определяется, главным образом, уровнем информационных технологий (от греч. τέχνη — искусство и *…логия*). В формальном смысле под *информационной технологией* понимается упорядоченная совокупность (ансамбль) методов переработки, изменения состояния, свойств, качественных видов и форм существования и проявления информации, а также способов тиражирования, распространения и хранения информации в процессе целенаправленной общественно-производственной деятельности [9].

Архитектура информационного права

Современная отрасль *информационного права* [7, 10] представляет собой исторически сложившуюся четырехкомпонентную систему, объединяющую в настоящее время следующие базовые развивающиеся подотрасли и институты:

- *право информационной безопасности* (включает институт информационных прав и свобод, институт тайны, институты охраны права на частную и публичную информационную деятельность и др.)[4];
- *медиаправо*, или право массовой информации (институт свободы массовой информации, институт прав телерадиовещателей и др.)[5];
- *компьютерное право* (институты электронного документооборота, электронной подписи, программно-математического обеспечения и др.)[6];
- *телематическое право,* или интернет-право, или сетевое право (институты телекоммуникаций и связи, институт доменных имён и др.)[7],

регулирующие определенные группы видов информационных отношений в информационной сфере (инфосфере) общественно-производственной деятельности.

Развиваются также отраслевые («общеподотраслевые») институты: права на информацию, информационно-правового режима и др. В последние годы в связи со стремительным развитием средств телематики и вычислительной техники возник и совершенствуется «межподотраслевой» институт «цифровых» прав (прав на цифровые данные, технологии, объекты интеллектуальной собственности [6, 13], криптовалюты[8], токены[9]) и др.

Цифровое право в широком смысле представляет собой совокупность правовых норм относительно доступа к использованию компьютеров, их сетей, сетей сотовой связи, цифровых медиа и глобальных телематических сетей[10].

Основой «цифровой экономики» — новой развивающейся мировой экономической деятельности, объединяющей, в первую очередь, *электронный бизнес* и *электронную коммерцию* (торговлю) и всё чаще использующей *электронные* (цифровые) *деньги* (включая криптовалюту — *Bitcoin*, *Litecoin* и др., всего более 800 разновидностей), защищаемые криптографическими способами — электронной цифровой подписью[11] и последовательным хэшированием[12], являются так называемые

---

[3] Например, представленной совокупностью значений скалярных показателей структурной сложности теоретико-графовых моделей технологических процессов целевого функционирования и топологии эргасистем, характеризующих их организованность и технологическую функциональность.

[4] *Ниесов В. А., Полякова Т. А., Стрельцов А. А., Чубукова С. Г.* Организационное и правое обеспечение информационной безопасности. М. : Юрайт, 2016.

[5] *Федотов М. А.* Право массовой информации в Российской Федерации. М. : Междунар. отношения, 2002.

[6] *Батурин Ю. М.* Проблемы компьютерного права. М. : Юр. лит-ра, 1991.

[7] *Наумов В. Б.* Право и Интернет: Очерки теории и практики. М. : Университет, 2002. *Голоскоков Л. В.* Теория сетевого права. М. : МПСУ, 1912.

[8] Термин «криптовалюта» (от англ. *cryptocurrency*) используется для определения *цифровых* денег, не эмитируемых в физическом виде, а для хранения соответствующих учетных записей в распределенной базе данных используется криптографическое шифрование. Хотя обычная («фиатная») валюта также оборачивается в виде *электронных* денег на кошельках электронных платежных систем и на банковских счетах, но ее эквивалентом выступают физические банкноты и монеты.

[9] Токен (от англ. *token* — жетон) — ключ или единица учета, предназначенная для представления цифрового баланса в некотором активе, выполненные в виде компактного устройства (например, USB-брелока).

[10] В российском законодательстве понятие *цифровое право* трактуется значительно уже — пока только в экономическом смысле. Согласно поправкам в Гражданский кодекс, вступившим в силу 1 октября 2019 г., *цифровые права* — это обязательственные и иные права, содержание и условия осуществления которых определяются правилами конкретной информационной системы (ст. 141.1 ГК РФ).

[11] Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» // Российская газета. 2011. 8 апр.

[12] *Хэширование* (от англ. *hashing* — крушить, расставлять) — преобразование («расстановка», «окрошка») по определённому алгоритму сообщения — массива исходных или входных данных в выходную битовую строку установленной длины («сводку сообщения», «хеш», «хеш-код», «хеш-сумму»).

телематические (информационно-компьютерные технологии телекоммуникаций) или «цифровые» технологии.

Цифровые технологии подразделяются на три основные класса:

- производства цифровой информации (содержательной информации в электронно-цифровой форме — в форме *цифровых данных*), включая рецепцию, генерацию, селекцию, измерение, классификацию, распознавание; моделирование и др.;
- интерпретации цифровой информации, включая преобразование, логическую обработку и аккумуляцию (в тезаурусе — исходном запасе знаний получателя);
- коммуникации цифровой информации в глобальных телематических сетях (ГТС) типа Интернет, Релком, Ситек, *Sedab*, *Remart* и др., включая передачу, хранение и предоставление.

Собственно *цифровые данные*, имеющие правовую значимость, на сегодняшний день включают:

- документы (дипломы, аттестаты, сертификаты, приватизационные чеки и др.);
- ценные бумаги (криптовалюты, электронные деньги, векселя, акции, облигации, закладные и др.);
- результаты интеллектуальной деятельности (базы данных, программы для ЭВМ, произведения[13] литературы, искусства и науки, изобретения и др.).

В связи с этим развивающиеся так называемые «цифровые» права — это, по сути, права на *цифровые информационные объекты*, включая, главным образом, цифровые технологии и данные. Особенности цифровых прав определяются спецификой *объекта* цифровых правоотношений (информационных, информационно-гражданских, информационно-уголовных и др.), в качестве которого выступают рассмотренные цифровые информационные объекты, и спецификой ГТС, включая, в частности, неопределённость правового статуса последних, экстерриториальность и коллективность «сетевого» использования цифровых данных (цифровых объектов интеллектуальной собственности и др.), практическую сложность установления нарушителей, нечёткость определения применимой юрисдикции, необязательность регистрации информационных (цифровых) объектов авторских и иных прав, массовость и географическую распределённость доступа и др.

При этом *цифровые данные,* являющиеся одной из форм представления информации, и *электронно-цифровые средства* информационных технологий *материальны*, а содержательная информация (отражённое разнообразие, характеризующее снятую неопределённость) и информационные технологии (ансамбль математических методов переработки) — *идеальны* [8].

Отсюда объектами права, в частности, гражданских прав являются так называемые *цифровые информационные объекты* (т. е. размещённые в ГТС цифровые данные, криптовалюты, объекты интеллектуальной собственности [13]; электронно-цифровые средства информационных технологий, информационные технологии как программно-реализованное информационно-математическое обеспечение переработки информации и др.), но не сама содержательная информация или ансамбль математических методов.

В предметной области информационного права для формирования и развития научно-методической базы правового регулирования возникающих в информационной (цифровой) сфере новых информационных отношений используются следующие естественнонаучно-математические методы [11]:

- информационно-аксиологический (от греч. αξια — ценность) метод *правовой информологии*[14] — количественное оценивание качества правовой и иной содержательной информации, т. е. свойств информации, имеющих принципиальное значение для правового регулирования целевых информационных отношений, а также информационной эффективности (целевой и технологической) и информационной безопасности жизнедеятельности (функционирования) личности, общества и государства;
- информационно-технологический метод *правовой информатики* — количественное оценивание качества и эффективности применения информационно-компьютерных технологий и электронно-вычислительной (компьютерной) техники в сфере юридически значимой электронной деятельности (автоматизированного судопроизводства, электронного голосования, электронной коммерции и др.).

Стремительное развитие информационной (включая «цифровую») сферы общественно-производственной деятельности и существенное повышение доли цифровых технологий оказывают конструктивное влияние на отечественное правоведение (в первую очередь, в отношении перехода на системно-правовую парадигму на основе концептуально-логического и математического моделирования [5, 8, 10, 16]), право в целом и соответствующее законодательство.

Регламентация цифровых прав

Первым шагом реализации правового регулирования отношений в цифровой экономике России [2] явилось принятие Федерального закона от 18 марта 2019 г. № 34-ФЗ (*о цифровых правах*)[15], создающего основу для регулирования путем приравнивания *цифровой* формы сделки к письменной и признания смарт-контрактов

[13] Размещаемые, в частности, в инфосфере ГТС Интернет с присвоением **цифрового идентификатора объекта** или *DOI (Digital object identifier)* — современный стандарт обозначения представленной в сети Интернет информации об объекте (в том числе электронно-цифровом), используемый всеми крупнейшими международными научными организациями и издательствами. В настоящее время идентификатор *DOI* является наиболее надежным и всемирно признанным средством идентификации и поиска научных данных *(цифровых информационных объектов)*, размещенных в сети Интернет.

[14] Исследует природу социально-правовой информации и её связанность с самоорганизующейся правовой системой общества.

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

(«быстрых сделок»[16] в ГТС Интернет), а также определения порядка оборота цифровых данных, удостоверяющих права на объекты гражданских прав (вещи, иное имущество, результаты работ, оказание услуг, исключительные права), посредством регистрации в информационной системе. Юридически, в частности, согласно данному Федеральному закону:

- «цифровые права» отнесены к объектам гражданских прав (ст. 128 ГК РФ);
- определено понятие «цифровые права», дана характеристика и определен субъект правоотношений (ст. 141.1 ГК РФ);
- уточнено понятие «самоисполняемой сделки», выполняемой путем применения информационных технологий, определенных условиями такой сделки (ст. 309 ГК РФ);
- идентифицированы дистанционные сделки, осуществляемые с помощью электронных технических средств (ст. 434 ГК РФ);
- предусмотрены ограничения для использования электронных средств (ст. 1124 ГК РФ).

Под «самоисполняемой («быстрой») сделкой» предлагается понимать сделку, определенную в смарт-контракте. «*Смарт-контракт*» — это договор, существующий в форме *компьютерного протокол*а (программного кода), имплементированного на платформе цифровой технологии *блокчейн* (от англ. *block chain* — цепочка блоков), который обеспечивает автономность и самоисполнимость условий такого договора при наступлении заранее определенных в нем обстоятельств *без привлечения третьих лиц* [17, 21]. В частности, смарт-контракт, в котором записаны значения остатков на счетах держателей токенов, предоставляет возможность перевода токенов с одного счёта на другой. Основная часть современных токенов формируется на протоколе *Blockchain* от открытой блокчейн-платформы *Ethereum* (Эфириум)[17].

Дополнительно закон дал возможность *электронного голосования* (один из видов цифровых прав) по вопросам принятия решений в обществах.

К сожалению, дальше декларации возможности получения «цифровых прав» дело пока не пошло. Да и о самих цифровых правах (существуют в электронном виде) закон четко не говорит, а дает только их *экономическую* характеристику как *обязательственных* (т. е. прав требования) или *иных*, содержание и условия осуществления которых определяются *только* в соответствии с правилами конкретной (одной) информационной системы (без обращения к третьему лицу), то есть цифровые права вне информационной системы не существуют. Следовательно, к цифровым правам могут относиться *цифровые финансовые активы* (токены, криптовалюты и др.), выпускаемые конкретными компаниями, но классические криптовалюты, уже имеющие «хождение»[18] и в России — не могут!

Пока только банки, страховые компании и сотовые операторы смогут воспользоваться принятым законом и реально перейти на заключение договоров с клиентами и совершение юридически значимых действий в электронном виде, поскольку с идентификацией трудностей в настоящее время нет.

Прошел год, но все ещё не ясно, что будет дополнительно отнесено к цифровым правам (токены, криптовалюты?), не ясна также система налогообложения при переходе цифровых прав.

Вместе с тем, как показывает практика, развитие цифровой экономики в России невозможно без легализации криптовалюты в гражданском законодательстве, против которой жестко выступает Центральный банк РФ (видимо, не исключает утопической идеи перспективного вытеснения криптовалютными блокчейн-компаниями классических банков из процесса кредитования — главного банковского процесса [3]). Но хотя *Bitcoin* (от англ. *bit* — бит и *coin* — монета) и был создан в противовес централизованной финансовой системе с её фиатными (традиционными) валютами, все равно представляется необходимым разработать комплекс регламентов, который сделал бы использование классической криптовалюты более безопасным, определил порядок взаимодействия *ICO* (от англ. *Initial Coin Offering* — «первичное предложение или размещение монет»[19]) криптовалют с другими юрисдикциями, приобретения токенов и криптовалют за рубежом. Это будет способствовать регуляции и благоприятному инвестиционному климату и не приведет к массовой миграции инвесторов, майнеров (валидаторов) блокчейн-платформ и предпринимателей, хотя бы на начальном этапе посредством разрешения обмена *цифровых финансовых активов* на рубли для совершения финансовых операций на территории Российской Федерации.

Информационная безопасность блокчейн-систем

С точки зрения информационного права основным вопросом легализации оборота цифровых финансовых активов и иных ценностей, а также заключения трансграничных сделок и др. является эффективность правового регулирования *информационной безопасности* [3, 12, 13] участников финансовых и коммерческих операций, использующих технологию блокчейн («распределенного реестра»), которая считается пока практически безопасной. При этом значительно повышается роль *индивидуального правового регулирования* [5] в связи с невозможностью подробного и адекватного нормативного описания всех возникающих в цифровой сфере динамических информационно-экономических и информационно-финансовых отношений.

Современные блокчейн-технологии, первоначально (в 2009 г.) созданные исключительно для *оперативного* децентрализованного (без доверенных посредников и

[16] Купли-продажи (через интернет-магазин и др.), дарения, залога и др.

[17] Интерес к блокчейн-платформе Эфириум проявили, в частности, Сбербанк и банк ВТБ.

[18] В середине 2019 г. на российский крипторынок вышла международная блокчейн-платформа *Puxful* для торговли биткоинами, объем торговли которой за прошлый год превысил 1,6 млрд долларов США. URL: www.decenter.org .

[19] Форма привлечения инвестиций в виде продажи инвесторам фиксированного количества новых единиц криптовалют, полученных разовой или ускоренной эмиссией.

ненужных звеньев) электронного обращения криптовалюты (*Bitcoin* или биткоин), широко используются в ГТС в различных сферах экономики и социальной сферы (включая электронную коммерцию, банковскую сферу [3], госуправление [18], страхование, здравоохранение и др.)[20], поскольку обладают рядом преимуществ, в том числе и в отношении *живучести* (информационно-физической безопасности) и повышенной *информационной защищенности*. Это обусловлено тем, что блокчейн-технологии, наряду с использованием электронных цифровых подписей и мультиподписей, используют последовательно взаимосвязанные цепочки зашифрованных блоков данных, в частности, сетевых финансовых транзакций (записей), хранимых одновременно у всех независимых участников (простых пользователей и майнеров — создателей блоков) блокчейн-систем, поэтому «взлом» системы (т. е. географически распределённо хранимого множества взаимодействующих идентичных копий единой базы данных) чрезвычайно затруднен. А взламывать каждый зашифрованный блок (содержит заголовок, *метку времени,* ключи и хеш-коды текущего и предыдущего блоков для обеспечения связности и целостности, набор записей-транзакций) и множество его копий, которые хранятся в разных местах, достаточно долго и дорого. Причем каждая попытка взлома любого блока из цепочки обязательно будет замечена другими участниками блокчейн-системы. Да и физически разрушить блокчейн-систему практически невозможно в связи с использованием значительного числа узлов (компьютеров) для хранения копий с интерфейсами для доступа и подробной документацией, часто территориально «разбросанных» по всему миру.

Вместе с тем проблема *гарантированного* обеспечения *информационной безопасности* [12] блокчейн-систем остается актуальной, о чем, в частности, свидетельствуют результаты исследования применения технологии блокчейн в США — суммарный ущерб американских компаний вследствие использования «врожденных» информационных уязвимостей эксплуатируемых блокчейн-систем и соответствующих децентрализованных сетей составил в 2011—2018 гг. около 1 млрд долларов США[21].

Все блокчейн-системы обладают как *общими* информационными уязвимостями, определяемыми несовершенством традиционных и предлагаемых стандартизирующей международной организацией (СМО) *IETF* (*Internet Engineering Task Force* — Инженерный совет Интернета) модифицированных сетеобразующих протоколов ГТС, так и *специфическими*, определяемыми особенностями децентрализованных сетей. Кроме того, проблема *гарантированной* информационной безопасности усугубляется возможностью несанкционированного доступа к хранимым и циркулирующим привилегированным данным с использованием «популярных» с конца 90-х гг. *нетрадиционных информационных каналов* («скрытых»[22], «сублимографических» и др.). Например, в результате несанкционированного воздействия на протокол *глобальной динамической маршрутизации BGP* (англ. *Border Gateway Protocol* — протокол пограничного шлюза) возможно изменение маршрутов передачи привилегированных данных с выходом из контролируемой зоны для их сбора и содержательного анализа (криптоанализа), что может остаться незамеченным для взаимодействующих абонентов используемого сегмента ГТС.

При несанкционированном воздействии на протокол *разрешения доменных имен DNS* (англ. *Domain Name System* — система доменных имен) и искажении таблиц *IP*-адресов (необходимых для трансляции символьных доменных имен) ряда серверов возможна задержка и даже потеря передаваемых сообщений, а также их замена и инфильтрация нелегитимных данных[23].

Основные специфические «врожденные» информационные уязвимости блокчейн-систем связаны, в первую очередь, с их же достоинствами, и в первую очередь — с децентрализованностью, транспарентностью и псевдоанонимностью [21].

Децентрализованные (распределенные) регулирование, контроль и аудит, осуществляемые самим сетевым сообществом участников (без посредников — внешнего администратора, нотариусов и др.), не исключают возможность так называемой «атаки 51%» («*картельный сговор*»), когда организованная группа участников, сконцентрировав в своих руках 51% вычислительных мощностей блокчейн-систем, может начать действовать в своих интересах, подтверждая только выгодные для себя транзакции и/или затягивая подтверждение транзакций других участников, а также осуществлять откат транзакций, создавая альтернативные блоки и гарантированно опровергая то, что происходит в исходном реестре. При этом (а также в других непредвиденных обстоятельствах) защитное «отключение» сразу всей блокчейн-системы не представляется возможным из-за отсутствия центрального хаба (компьютера).

Транспарентность и публичная доступность базы данных (реестра) блокчейн-систем, обеспечивая в целом открытость системы (любой желающий может увидеть

[20] В частности, Центральный банк РФ вместе с рядом крупных банков создали в 2019 г. первую сертифицированную платформу «Мастерчейн», которая использует российские стандарты криптографии; в Москве функционирует блокчейн-платформа «Активный гражданин», созданы и функционируют частные платформы: кибер-Фонд (cyberFund), Сатоши_Фонд (Satoshi Fund), ГОЛОС (GOLOS) и др.

[21] *См. : Madnick S.* Blockchain is unbreakable? Think again. The Wall Street Journal, 2019, 6 june. [Электронный ресурс] URL: http://blogs.wsj.com/experts/2019/ (дата обращения 14.04.2020).

[22] *См.:* ГОСТ Р 53113.1-2008. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. М. : Стандартинформ, 2008. Исполн. *Д. Б. Кабелев, А. А. Грушо, А. В. Гусев, Д. А. Ловцов* и др.; ГОСТ Р 53113.2-2009. Информационная технология. Защита ИТ и АС от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, ИТ и АС от атак с использованием скрытых каналов. М. : Стандартинформ, 2009. Исполн. *Д. Б. Кабелев, А. А. Грушо, А. В. Гусев, Д. А. Ловцов* и др.

[23] Для атак такого рода все возможности имеются, поскольку управление корневой (*root*) зоной *DNS* осуществляет американская организация *ICANN* (*Internet Corporation for Assigned Names and Numbers* — Международная корпорация по присвоению имен и номеров), а техническое сопровождение работ по созданию и наполнению зоны осуществляет американская компания *Verisign, Inc.* (г. Рестон, штат Вирджиния), поддерживающая разнообразные сетевые структуры, включая два из тринадцати существующих (все — за рубежом) корневых серверов *DNS*.

историю всех транзакций) и, как следствие, снижение рисков коррупции, добросовестность финансовой, коммерческой и др. профессиональной деятельности независимых участников системы, не защищает от возможности криптоанализа математических «дефектов» (изъянов, «слабостей», уязвимостей) открытых ключей, кодов и возможных алгоритмов шифрования доступных блоков (транзакций), осуществляемого как самими участниками, так и высококвалифицированными злоумышленниками. Существует вероятность подбора закрытого ключа на основе алгоритмов, позволяющих эффективно факторизовать эллиптические[24] кривые и, возможно, если верить иностранным источникам, существуют вычислительные возможности обеспечения обратимости стандартизованных функций зашифрования[25].

Псевдоанонимность участника, осуществляющего зарегистрированные и доступные операции в автономной блокчейн-системе, обеспечивая его личную тайну как оператора (поскольку вместо персональных данных используется только уникальный номер или адрес кошелька, получаемые при регистрации в системе), не позволяет восстанавливать его доступ к своей учетной записи в случае утери (в том числе и в результате хищения) им своего закрытого ключа.

То есть человеческий фактор продолжает играть существенную роль в информационной безопасности любых информационных систем, включая блокчейн-системы, которые, как видно, не всегда защищены от злоупотреблений самих пользователей. В частности, уровни *взаимного доверия* людей в разных странах очень различаются: от 10% в Аргентине до 70% в Швеции[26] и могут резко колебаться в связи с изменениями морали в обществе и ухудшением социально-экономической ситуации. И остаются также открытыми вопросы: кто в блокчейн-системе отвечает за информационную безопасность, за мониторинг защищенности РТС и реагирование на инциденты, нужны ли какие-то стандарты независимым участникам для обеспечения равноправия в системе и др.?

Цифровая трансформация инфосферы

Для продуктивного мониторинга правоприменения в цифровой сфере (включая количественную оценку) и обеспечения эффективности функционирования национальных систем правового регулирования (правовых эргасистем) представляется целесообразным формирование *единого информационно-цифрового пространства* (ЕИЦП) как виртуальной области активного процессуального электронного взаимодействия работников (представителей, деятелей, персонала) и пользователей (участников, наблюдателей, граждан) сообщества правовых эргасистем на основе *цифровой трансформации* [6, 11] существующей инфосферы (см. *рисунок*) правоохранительной деятельности, включающей соответствующую *информационную среду,* функционирующую на базе национальной *информационной инфраструктуры,* информационно-технические средства, информационно-компьютерные технологии и организационно-юридические структуры правовых эргасистем для целесообразной переработки правовой *информации* [9].

При этом «цифровое» пространство — это составная часть информационного пространства, возникающая на основе функционирующей цифровой среды (части информационной среды), базирующейся на цифровой инфраструктуре (телематические системы и сети, хранилища и базы данных и знаний, электронные книги и др.), и объединяющая совокупность виртуальных *цифровых полей*, возникающих на основе функционирования соответствующих *цифровых площадок* (включающих цифровые средства и технологии определенных социальных групп, поддерживающих цифровые интернет-коммуникации) [4, 11].

Информационные деятели (см. *рисунок*) — источники и потребители информации ***A*** и ***B*** (включая «цифровые» *группы интернет-пользователей*) взаимодействуют посредством определенной информационной среды (*цифровых площадок*) и соответствующего информационного пространства (*цифровых полей*).

Под *информационной инфраструктурой* понимается совокупность правовых автоматизированных информационных систем (АИС), коммуникаций (информационно-телекоммуникационные и телематические сети), информационных ресурсов (информации библиотек, архивов, хранилищ и баз данных и знаний (БДЗ) и др.), находящихся в ведении государства.

Информационно-технические средства включают АИС правоохранительных органов, корпоративные и локальные информационно-вычислительные сети, информационно-правовое обеспечение (нормативно-правовые БДЗ, технологии их ведения и использования), информационно-лингвистическое обеспечение (классификаторы, словари, тезаурусы).

Информационная среда и соответствующее ЕИЦП *правоприменительной системы* формируются на основе единых принципов и общих правил с осуществлением мероприятий по включению информационных ресурсов судов, органов судейского сообщества и Судебного департамента при Верховном Суде РФ в объединенные БДЗ, интернет-сайты (порталы) и установлением единых требований к их созданию, функционированию, обеспечению доступа к *судебной информации*[27], а также к их эксплуатационному обслуживанию и развитию [14, 15].

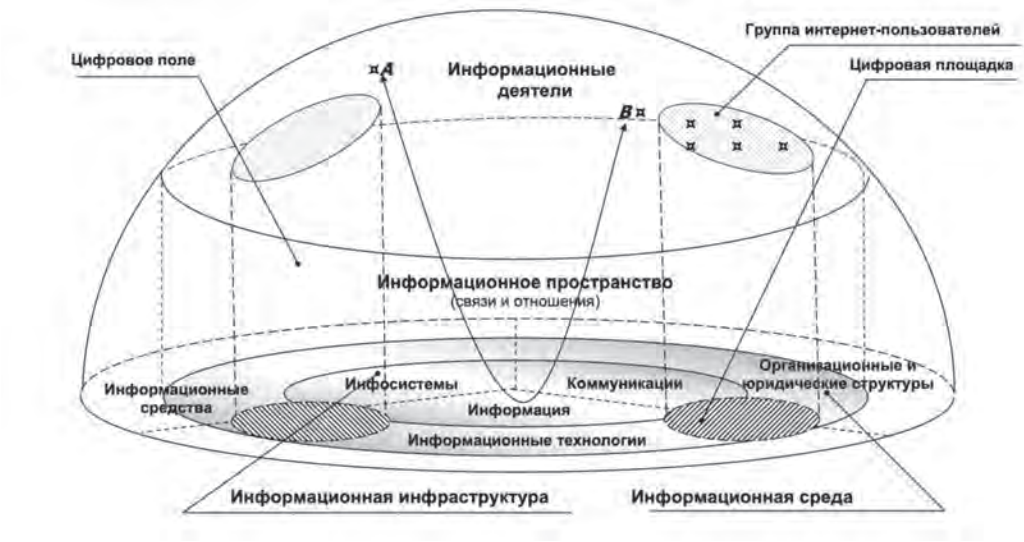
---

[24] Все отечественные ГОСТ семейства 34.10 основаны на использовании математических операций в группе точек эллиптической кривой над конечным полем вычетов по модулю большого простого числа.

[25] *См.: Wang Z., Yu H., Wang X.* Cryptanalysis of GOST R Hash Function // Tsinghua University (China), 2013. 11 p. [Электронный ресурс] URL: http://eprint.iacr.org.2013/584.pdf (дата обращения 05.05.2020).

[26] *См., например:* Исследование GfK Verein: Международный рейтинг уровня доверия в 2011 г. [Электронный ресурс] URL: https://gtmarket.ru/news/state/2011/12/21/3770 (дата обращения 11.10.2019).

[27] К *судебной информации* относятся сведения, возникающие в результате непосредственной деятельности органов судебной власти по организации и осуществлению судопроизводства, а также сведения о фактах и лицах, относительно их участия в судопроизводстве. Например, сведения об участниках (судьях, подсудимых, истцах, ответчиках и др.) судебного процесса, о сущности правового спора, о назначенных сроках рассмотрения дела и др.; судебные решения (обвинительные заключения, приговоры, постановления, определения и



Концептуально-логическая модель инфосферы

На современном этапе создания и развития ЕИЦП правовых эргасистем представляется целесообразной разработка *комплексного плана* интеграции АИС правоохранительных органов (Генпрокуратуры, МВД, судебной системы[28] и др.) со следующими государственными системами и сервисами в сфере обеспечения правового регулирования:

- система МЭДО и СМЭВ;
- единая системая нормативной справочной информации (для доступа к общегосударственным справочникам, классификаторам, реестрам, регистрам, словарям);
- информационный платёжный шлюз (для оплаты пошлин);
- единая система идентификации и аутентификации (для авторизации субъектов и объектов взаимодействия);
- единый Портал государственных услуг (для доступа граждан и судов к информации федеральных и региональных органов власти, в том числе к информации на «цифровых картах»[29]);
- информационно-справочные правовые и учётные системами министерств и ведомств;
- государственная почтовая система (для пересылки повесток судов, жалоб и предложений от граждан, в том числе с использованием SMS);
- системы дистанционного повышения квалификации работников правоохранительных органов в сфере правоприменения и др.

Для осуществления интеграции правовых АИС с элементами инфраструктуры «электронного правительства» представляется также целесообразным в рамках Государственной программы[30] РФ «Информационное общество» (2011—2020 гг.) спланировать и организовать разработку нормативно-методической базы формирования и развития ЕИЦП правовых эргасистем, обеспечивающего информационное взаимодействие правоохранительных органов между собой и с федеральными органами исполнительной власти в электронно-цифровом виде.

Создание и развитие ЕИЦП правовых эргасистем России представляет собой сложную комплексную научно-прикладную *проблему*. Ее решение сопряжено с выполнением широкого круга сложных системных задач организационно-правового обеспечения [6, 15, 16] процессов информатизации (цифровизации) правоохранительных органов и представляется возможным при объединении усилий и ресурсов заинтересованных государственных структур в рамках, например, перспективной целевой программы развития правоохранительной системы с учётом целей и задач формирования нового — информационного общества и его электронных и цифровых структур.

В частности, для модернизации *цифрового (автоматизированного) судопроизводства* такими системными задачами являются:

1) создание экосистемы цифрового судопроизводства, в которой данные в цифровой форме являются ключевым фактором его комплексного обеспечения;

др.), судебные исполнительные документы, справочные сведения (судебная статистика, обзоры судебной практики, интервью с работниками судебной системы по вопросам судопроизводства и др.).

[28] Включая АИС высших судов страны (Конституционного Суда РФ и Верховного Суда РФ), АИС судов общей юрисдикции и органов Судебного департамента при Верховном Суде РФ (ГАС РФ «Правосудие») и арбитражных судов (Единая автоматизированная информационно-коммуникационная система), а также комплексы средств автоматизации конституционных (уставных) судов и мировых судей субъектов Российской Федерации, их сайтов (порталов), систем связи и передачи данных.

[29] Цифровые (электронные) карты, а также объемные модели местности (3D-модели) и спутниковые фотографии, снабженные подробными комментариями и разъяснениями, удобны для наглядной экспликации результатов различных аналитических, исследовательских и научных работ. Находятся под защитой авторских прав.

[30] Утв. распоряжением Правительства РФ от 20 октября 2010 г. № 1815-р. Содержит 4 подпрограммы, одна из которых — «Информационное государство».

2) развитие системы российских центров переработки больших данных, которая обеспечивает предоставление государству, бизнесу и гражданам доступных, безопасных и экономически эффективных услуг по хранению и переработке данных;
3) внедрение цифровых платформ работы с данными;
4) создание эффективной системы сбора, обработки, хранения и предоставления потребителям *пространственных* данных [18];
5) обеспечение организационной и правовой защиты информационных (цифровых) ресурсов.

Как видно, каждая из пяти системных задач способствует формированию комплексного проекта создания информационной инфраструктуры цифрового судопроизводства.

В современных условиях формирования и развития информационного общества практически все государственные структуры, участвующие в сфере правоприменения (судопроизводства), все больше ощущают свою зависимость от качества правового регулирования отношений в сфере цифровых технологий судопроизводства на межведомственном уровне. Например, на различных стадиях судопроизводства деятельность правоохранительных и судебных органов, следственных органов, органов прокуратуры, нотариата, структур исполнительного производства, государственных судебно-экспертных учреждений, инспекций Федеральной налоговой службы и иных структур, обеспечивающих судопроизводство, поддерживается большим числом разрозненных *автоматизированных систем*, не имеющих системно разработанного нормативного организационно-правового обеспечения их совместного функционирования и развития.

Заключение

Таким образом, рассмотрены общие информационно-правовые основы правоприменения в цифровой сфере, а также состояние и пути имплементации цифровых прав на научно-методической базе современной теории информационного права, в частности:

- определены специфические объекты целевых информационных правоотношений (информационных правоотношений в инфосфере), в качестве которых рассматриваются компоненты информационной деятельности в инфосфере;
- рассмотрена система, актуальные цифровые объекты и специальные методы современного информационного права, при этом классифицированы (по виду информационных процессов) реальные цифровые технологии;
- исследовано состояние правовой регламентации «цифровых прав» в России и уровень информационной безопасности блокчейн-технологии;
- определено состояние и пути решения проблем цифровой трансформации инфосферы с целью обеспечения эффективности мониторинга правоприменения в цифровой сфере, при этом уточнена концептуально-логическая модель инфосферы.

Обоснованы также следующие *выводы*, имеющие прагматическое значение:

- об объективности тенденции концептуального перехода в отечественном правоведении к системно-математическим представлениям о праве, что соответствует общемировой тенденции в условиях глобальной цифровой информатизации;
- о невозможности развития цифровой экономики в России без легализации криптовалюты в гражданском законодательстве;
- о неочевидности информационной безопасности блокчейн-технологии, в первую очередь, в силу существования возможности злоупотреблений самих пользователей;
- о необходимости межведомственного развития единого информационно-цифрового пространства правовых эргасистем России и коллективной разработки нормативного организационно-правового обеспечения совместного функционирования и развития разрозненных ведомственных АИС, участвующих в процессе правоприменения, с учётом целей и задач формирования нового — информационного — общества.

Литература

1. Бачило И. Л. Информационное право. М.: Юрайт, 2011.
2. Вайпан В. А. Основы правового регулирования цифровой экономики // Право и экономика. 2017. № 10. С. 5—18.
3. Ващекин А. Н., Ващекина И. В. Противодействие преступной деятельности в условиях развития цифровых технологий дистанционного банковского обслуживания // Правовая информатика. 2019. № 4. С. 86—95. DOI: 10.21681/1994-1404-2019-4-86-95.
4. Ващекин А.Н., Дзедзинский А.В. Правовое регулирование отношений в цифровом пространстве // Правосудие. 2020. № 3. С. 108—114.
5. Ершов В. В. Правовое и индивидуальное регулирование общественных отношений: Монография. М.: РГУП, 2018. 628 с. ISBN 978-5-93916-631-7.
6. Карцхия А. А. Цифровая трансформация права // Мониторинг правоприменения. 2019. № 1(30). С. 25—29. DOI: 10.21681/2226-0692-2019-1-25-29.
7. Ловцов Д. А. Теория информационного права: базисные аспекты // Государство и право. 2011. № 11. С. 43—51. ISSN 0132-0769.
8. Ловцов Д. А. Системология правового регулирования информационных отношений в инфосфере: архитектура и состояние // Государство и право. 2012. № 8. С. 16—25. ISSN 0132-0769.
9. Ловцов Д. А. Информационная теория эргасистем: Тезаурус. М.: Наука, 2005. 248 с. ISBN 5-02-033779-X.
10. Ловцов Д. А. Системологические основы эффективного правового регулирования информационных отношений в инфосфере // Мониторинг правоприменения. 2020. № 1(34). С. 37—44. DOI: 10.21681/2226-0692-2020-1-37-44.
11. Ловцов Д. А. Эффективность правовых эргасистем в инфосфере // Правовая информатика. 2020. № 1. С. 4—14. DOI: 10.21681/1994-1404-2020-1-04-14.
12. Ловцов Д. А. Проблема гарантированного обеспечения информационной безопасности крупномасштабных автоматизированных систем // Правовая информатика. 2017. № 3. С. 66—74. DOI: 10.21681/1994-1404-2017-3-66-74.
13. Ловцов Д. А., Галахова А. Е. Защита интеллектуальной собственности в сети Интернет // Информационное право. 2011. № 4. С. 13—20.
14. Ловцов Д. А., Ниесов В. А. Актуальные проблемы создания и развития единого информационного пространства судебной системы России // Информационное право. 2013. № 5. С. 13—18.
15. Ловцов Д. А., Ниесов В. А. Проблемы и принципы системной модернизации «цифрового» судопроизводства // Правовая информатика. 2018. № 2. С. 15—22. DOI: 10.21681/1994-1404-2018-2-15-22.
16. Мацкевич И. М. Интеллектология права. Предварительные итоги математического моделирования закона // Мониторинг правоприменения. 2019. № 1(30). С. 4—15. DOI: 10.21681/2226-0692-2019-1-04-15.
17. Савельев А. И. Некоторые аспекты использования смарт-контрактов и блокчейн-технологий по российскому праву // Закон. 2017. № 5. С. 94—117.
18. Черных А. М. Защищенность данных об объектах недвижимости и земельных ресурсах на базе геоинформационных и блокчейн технологий // Правовая информатика. 2019. № 4. С. 75—85. DOI: 10.21681/1994-1404-2019-4-75-85.
19. Craig B. CyberLaw: The Law of the Internet and Information Technology. Paperback, 2012.
20. Ferrera G. R., Reder M. E. K. CyberLaw: Text and Cases. Paperback, 2011.
21. Franco P. The Blockchain. Understanding Bitcoin: Cryptography, Engineering and Economics. John Wiley & Sons, 2014. 288 p. ISBN 978-1-119-01916-9.

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