УДК 004.9, 003.26, 004.056, 34.096
DOI: 10.33764/2618-981X-2019-9-42-46

ПОСТРОЕНИЕ ЮРИДИЧЕСКИ ЗНАЧИМОГО ЗАЩИЩЕННОГО ДОКУМЕНТООБОРОТА НА ОСНОВЕ БЛОКЧЕЙН В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Любовь Денисовна Заворина
Новосибирский государственный университет экономики и управления, 630099, Россия, г. Новосибирск, ул. Каменская, 52/1, студент, тел. (913)746-00-96, e-mail: ljubasik-1234@mail.ru

Анастасия Алексеевна Ерохина
Новосибирский государственный университет экономики и управления, 630099, Россия, г. Новосибирск, ул. Каменская, 52/1, студент, тел. (913)488-50-46, e-mail: eroxina1997@bk.ru

Диана Георгиевна Макарова
Сибирский государственный университет геосистем и технологий, Россия, 630108, г. Новосибирск, ул. Плахотного, 10, старший преподаватель кафедры информационной безопасности, тел. (383)343-91-11, e-mail: kaf.ib@ssga.ru

В статье рассматривается проблема системы электронного документооборота с использованием технологии «Блокчейн» для государственных органов, а именно, для критической информационной инфраструктуры. Данная проблема является актуальной, поскольку развитие цифровой экономики в России уже достигло уровня правительства.

Ключевые слова: критическая информационная инфраструктура, блокчейн, цифровая экономика, информационная система.

BUILDING OF A LEGALLY SIGNIFICANT PROTECTED DOCUMENT MANAGEMENT BASED ON BLOCKCHAIN IN INFORMATION SYSTEMS

Lyubov D. Zavorina
Novosibirsk State University of Economics and Management, 52/1, Kamenskaya St., Novosibirsk 630099, Russia, Student, phone: (913)746-00-96, e-mail: ljubasik-1234@mail.ru

Anastasia A. Erokhina
Novosibirsk State University of Economics and Management, 52/1, Kamenskaya St., Novosibirsk, 630099, Russia, Student, phone: (913)488-50-46, e-mail: eroxina1997@bk.ru

Diana G. Makarova
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Senior Lecturer, Department of Information Security, phone: (383)343-91-11, e-mail: kaf.ib@ssga.ru

The article deals with the problem of electronic document management system using "Blockchain" technology for public authorities, namely for critical information infrastructure. The problem is relevant since the development of the digital economy in Russia has already reached the governmental level.

Key words: critical information infrastructure, blockchain, digital economy, information system.

Совсем скоро нас ждет эра цифровой экономики – системы экономических, социальных и культурных отношений, которая основана на инженерии компьютерных систем, математике и криптографии. Основной задачей цифровой экономики является улучшение качества жизни граждан.

Главное преимущество нововведения – математический алгоритм блокчейн, который позволяет вести надежный учет финансов, денежных расчетов, и даже операций с материальными и нематериальными активами. Эта уникальная технология делает возможным записать в цифру все то, что так важно человеку, безопасно хранить и передавать друг другу, минуя посредников. Благодаря глобальной бухгалтерской книге, которая позволяет фиксировать историю транзакций, стало невозможным подделать состояние счетов. Таким образом, в мире блокчейн доверие возникнет из сети.

Первоначальное появление технологии блокчейн в качестве инструмента для проведения транзакций с электронной валютой «биткоин» получило развитие как обособленная технология, которая может использоваться за рамками криптовалют. В России (далее – РФ) она получила название технологии распределенного реестра (англ.: Distributed ledger technology – DLT).

Блокчейн обладает преимущественными функциями безопасности, а именно:

– защищенность (данные шифруются для подтверждения транзакций);

– неизменность (от предшествующих транзакций зависит текущее состояние блокчейн);

– прозрачность (обеспечивается публичным и распределенным хранением) [1].

Таким образом, технология блокчейн может способствовать защите государственных интересов.

В начале 2016 г. в Великобритании был опубликован отчет «Технология распределенных реестров: за рамками блокчейн», представляющий исследование, проведенное Государственным управлением науки под руководством главного научного советника Правительства Великобритании Ричарда Кастеляйна (Richard Kastelein). В отчете отмечается, что главная задача государства заключается в разработке четкой концепции того, как технология распределенных реестров может улучшить деловые процессы государственных органов, и каким образом она может быть использована для оказания услуг гражданам. Государство должно выступить в роли продвинутого заказчика, внедряющего эту технологию. Поступая таким образом, государство может поддерживать и влиять на развитие экономической активности в этом секторе.

По мнению специалистов, занимающихся анализом технических решений в области блокчейн-технологий, на данный момент существуют следующие возможные проблемы:

– обеспечение требуемой пропускной способности сети для нормальной работы блокчейна;

– предоставление узлу необходимого дискового пространства из-за непрерывной генерации блоков.

Для использования технологии блокчейн в государственной сфере должны быть внесены изменения в нормативно-правовые акты РФ в сфере информационных технологий. Для определения таких изменений, Минэкономразвития России 17 октября 2017 г. подготовило Проект Постановления Правительства РФ «О проведении на территории г. Москвы эксперимента по использованию технологии «Блокчейн» в целях мониторинга достоверности сведений Единого государственного реестра недвижимости». Целями эксперимента являются определение эффективности и результативности использования технологии блокчейн, определение изменений, которые необходимо внести в нормативно-правовые акты РФ в сфере информационных технологий, определение технических возможностей информационной системы по использованию технологии блокчейн.

Изменения могут коснуться Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», регулирующего отношения в области обеспечения безопасности критической информационной инфраструктуры РФ (далее – КИИ) в целях ее устойчивого функционирования при проведении в отношении нее компьютерных атак.

Объектами КИИ, согласно вышеупомянутому закону, являются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ. На данный момент идет определение точного перечня объектов КИИ. Одним из субъектов КИИ стали государственные органы, которым на праве собственности, аренды или ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления (например, Минздрав НСО) [2].

Если блокчейн включить в список объектов КИИ, то его безопасность будет регулироваться данным законом.

Так как, в блокчейн все операции совершаются над цифровыми объектами, то необходимы изменения в законодательстве о регулировании оборота цифровых прав и цифровых денег, для совершения и исполнения сделок в так называемой цифровой среде. 26 марта 2018 г. в Государственную Думу был внесен законопроект №424632-7 о внесении изменений в части первую, вторую и четвертую Гражданского Кодекса РФ (о цифровых правах). В соответствии с проектом закона под «цифровым правом» понимается совокупность электронных данных (цифровой код), которая удостоверяет права на объекты гражданских прав. Принятие законопроекта позволит не только закрепить отправные гражданско-правовые нормы для регулирования оборота цифровых прав и цифровых денег, совершения и исполнения сделок в так называемой цифровой среде, но и позволит решить целый ряд других задач. В частности, будет обеспечена судебная защита прав, возникающих в отношениях по поводу таких объектов.

Технологию блокчейн можно внедрить в работу государственных органов, таким образом, она (технология) заменит работу информационной системы.

Чтобы сделать работу блокчейн более эффективной и удобной, необходимо понять, как используется информационная система.

Важнейшее место в работе государственных органов занимает электронный документооборот, построенный с использованием цифровой подписи. Фактически, электронный документооборот – это обмен документами в электронном виде. Информация, которая циркулирует в государственных органах, может носить конфиденциальный характер, следовательно, попадая в общедоступную сеть, она нуждается в защите. Электронная подпись решает следующие задачи:

– защита документов от модификации и подделки;

– определение автора документа, а также подлинности документа;

– обеспечение юридической силы документов;

– защита документов от несанкционированного просмотра.

Система электронного документооборота может строиться с использованием технологии блокчейн. Для этого необходимо разработать распределенное приложение для государственных органов на блокчейн-платформе Ethereum. Ethereum – конструктор для создания решений на блокчейн [3].

Для того, чтобы внедрить распределенное приложение в информационные системы государственных органов, оно должно соответствовать требованиям ФСБ России и ФСТЭК России.

Для начала опишем требования к информационной технологии Электронная подпись (ЭП):

– показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;

– создавать ЭП только после подтверждения лицом, подписывающим электронный документ, операции по созданию ЭП;

– показывать информацию о внесении изменений в подписанный ЭП электронный документ;

– указывать на лицо, с использованием ключа ЭП которого подписаны электронные документы.

Теперь сформулируем требования к блокчейн по информационной безопасности для возможности применения в государственных органах [5–9]:

– сопоставление пользователя с устройством. Идентифицированная система (приложение) должна включать в себя механизм, посредством которого санкционированный пользователь надежно сопоставляется с выделенным устройством [2];

– аутентификация и идентификация. Система должна требовать от пользователей идентифицировать себя при запросах на доступ и подвергать проверке подлинность идентификации – осуществлять аутентификацию;

– использование ассиметричного механизма электронной подписи для работы в приложениях на основе блокчейн. Данное требование устранит возможность использования пользователями сотен открытых ключей;

– документ, заверенный электронной подписью, должен читаться только при использовании ключа;

– открытый ключ (электронная подпись) должен передаваться вместе с документом.

БИБЛИОГРАФИЧЕСКИЙСПИСОК

1. МеланиСвон (MelanieSwan). Блокчейн. Схема новой экономики (Blockchain: Blueprintfora New Economy). – М: Олимп-Бизнес, 2016. – 240 с.

2. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа кинформации», утвержденный решением председателя Государственной техническойкомиссии при Президенте Российской Федерации от 30 марта 1992 г.

3. Тапскотт Дон, Тапскотт Алекс. Революция блокчейн. Как технология, стоящая за биткоин, меняет деньги, бизнес и мир. – М: SmartReading, б.г. – 20 с.

4. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.

5. Селифанов В. В., Звягинцева П. А., Юракова Я. Ю. Применение методов автоматизации при определении актуальных угроз безопасности информации в информационных системах с применением банка данных угроз ФСТЭК России // Вестник СГУГиТ. – 2017. – Т. 22, № 4. – С. 202–209.

6. Селифанов В.В. Оценка эффективности системы защиты информации государственных информационных систем от несанкционированного доступа [Текст] // Интеграция науки, общества, производства и промышленности: сборник статей Международной научно-практической конференции, 2016. – С. 109–113.

7. Оценка эффективности системы защиты информации ИСПДН с учетом профиля защиты / В. В. Селифанов, П. А. Звягинцева, А. С. Голдобина, Ю. А. Исаева // Вестник СГУГИТ. – 2017. – Т. 22, № 4. – С. 220–225.

8. Селифанов В.В., Ремизова В.А. Проведение аттестационных испытаний средств антивирусной защиты // Информационные системы и процессы, сборник научных трудов, Новосибирский государственный университет экономики и управления «НИНХ» (Новосибирск), 2015. – С. 208–213.

9. Селифанов В.В., Курносов К.В. Требования к системе защиты информации для виртуальной инфраструктуры // Информационное противодействие угрозам терроризма. – 2014. – № 23.– С. 188.