

Секция «Правовая информатика, информационное и цифровое право»

Алгоритмическое правосудие: правовые вызовы внедрения DLP-систем в блокчейн-технологии для защиты коммерческой тайны

Научный руководитель – Беларева Ольга Александровна

Глушков Валентин Алексеевич

Студент (бакалавр)

Новокузнецкий филиал-институт Кемеровского государственного университета,
Факультет истории и права, Новокузнецк, Россия

E-mail: valekpike@gmail.com

В данной работе рассматриваются правовые вызовы, возникающие при внедрении систем предотвращения утечек данных (DLP) в блокчейн-технологии, используемые для защиты коммерческой тайны. Значимость исследования обусловлена растущей цифровизацией деловых процессов, расширением сферы применения распределенных реестров и необходимостью обеспечения надежной защиты конфиденциальной информации. Анализируются ключевые преимущества DLP-систем в контексте блокчейна, включая неизменяемость данных и децентрализованное управление, а также выявляются правовые проблемы, связанные с обеспечением конфиденциальности, аутентификации, соблюдением прав субъектов данных и юридической ответственностью. Представлен обзор нормативно-правовой базы, регулирующий использование блокчейн-технологий и информационной безопасности, а также выявлены коллизии, требующие законодательных инициатив для устранения правовой неопределенности.

Современное развитие алгоритмического правосудия основывается на внедрении автоматизированных решений, использующих технологии искусственного интеллекта (ИИ) и машинного обучения. Блокчейн и DLP-системы являются неотъемлемыми компонентами данных процессов, поскольку они обеспечивают неизменяемость записей, криптографическую защиту информации и контроль над возможностью утечек данных. Однако правоприменительная практика сталкивается с проблемами, связанными с прозрачностью алгоритмических решений, защитой персональных данных и нормативным регулированием таких технологий.

Блокчейн-системы характеризуются децентрализованной природой, высокой степенью защиты от манипуляций и автоматизированным управлением данными посредством смарт-контрактов. Их использование в правовой сфере потенциально снижает коррупционные риски, упрощает процесс верификации и хранения юридически значимой информации. Однако неизменяемость записей блокчейна вступает в противоречие с некоторыми нормативными требованиями, в частности с принципами защиты персональных данных и правом на забвение, закрепленным в Общем регламенте ЕС по защите данных (GDPR)[1].

DLP-системы предназначены для предотвращения несанкционированного распространения конфиденциальной информации. Они включают механизмы мониторинга сетевого трафика, анализа содержимого данных, управления инцидентами и контроля конечных устройств. Интеграция DLP с блокчейном позволяет использовать интеллектуальные контракты для управления доступом и фиксации операций с данными, что обеспечивает дополнительный уровень безопасности. Однако правоприменение данных технологий требует уточнения нормативных положений, касающихся разграничения ответственности между субъектами обработки информации.

Юридические вопросы, возникающие в связи с использованием блокчейна и DLP, касаются соблюдения требований по конфиденциальности и защите данных. В условиях

децентрализованных систем управление доступом к информации затруднено, а возможность модификации данных отсутствует. Это создает вызовы для соблюдения прав субъектов данных, например, при необходимости удаления информации. В качестве возможных решений рассматриваются методы криптографической защиты, включая доказательства с нулевым разглашением, обеспечивающие конфиденциальность данных при сохранении прозрачности их обработки.

Ответственность за решения, принятые на основе алгоритмических систем, остается нерегулированной областью. При наличии ошибок в DLP- или блокчейн-системах, затрагивающих права субъектов данных, возникают вопросы о распределении юридической ответственности между разработчиками, операторами системы и пользователями. В ряде стран, например в США, уже применяются судебные прецеденты, касающиеся ответственности за предвзятость и ошибки алгоритмов[2]. В российском правовом поле аналогичные вопросы пока остаются без четкого регулирования.

Существующее законодательство, включая Федеральные законы № 152-ФЗ «О персональных данных»[3] и № 98-ФЗ «О коммерческой тайне»[4], требует соблюдения норм защиты конфиденциальной информации. Однако децентрализованная архитектура блокчейна усложняет идентификацию ответственных лиц, поскольку управление данными осуществляется распределенно, без единого центра. Это создает правовую неопределенность, которая требует разработки новых механизмов регулирования.

Практика использования блокчейна уже находит применение в таких сферах, как финансовый сектор, интеллектуальная собственность, медицинские базы данных и государственные реестры. Например, в некоторых странах технология используется для ведения кадастровых реестров, что обеспечивает их неизменяемость и снижает вероятность мошенничества. Однако адаптация нормативных актов к таким технологиям пока находится на ранней стадии, что создает потенциальные юридические риски.

На международном уровне регулирование блокчейна и DLP-систем осуществляется в разных направлениях. В ЕС акцент делается на защиту персональных данных и соблюдение требований GDPR, в США внимание сосредоточено на финансовом регулировании и борьбе с отмыванием денег. В России нормативно-правовая база по вопросам использования DLP-систем в блокчейне требует уточнения, в частности в части соответствия требованиям законодательства о защите информации.

Интеграция DLP-систем в корпоративные и государственные процессы позволяет минимизировать угрозы утечек данных, однако их сочетание с блокчейном требует разработки дополнительных механизмов мониторинга и контроля. Поскольку распределенный реестр не предусматривает возможности удаления или изменения записей, необходимо учитывать риски, связанные с сохранением потенциально устаревшей или недостоверной информации. Разработка алгоритмов динамического управления доступом могла бы частично решить данную проблему, однако их применение в распределенных системах требует правового закрепления.

Для эффективного правового регулирования внедрения DLP-систем в блокчейн-технологии необходимо разработать нормативные стандарты, определяющие баланс между конфиденциальностью данных и требованиями к их прозрачности. Важной задачей является формирование юридических механизмов распределения ответственности между участниками блокчейн-сетей, разработчиками алгоритмов и пользователями систем. Внешение изменений в действующее законодательство, адаптация норм к специфике распределенных систем и разработка стандартов по обработке данных в децентрализованных структурах являются ключевыми направлениями правового развития данной области.

Использование блокчейна и DLP-систем для защиты коммерческой тайны представляет собой значительное технологическое достижение, однако требует комплексного подхода

к нормативному регулированию. Важно разработать эффективные правовые механизмы, обеспечивающие баланс между прозрачностью операций, защитой конфиденциальности и соблюдением прав субъектов данных. В перспективе исследование правовых аспектов интеграции DLP в блокчейн позволит сформировать более устойчивую модель регулирования цифровых данных, способствующую развитию безопасных и эффективных технологий обработки информации.

Источники и литература

- 1) О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31.07.2020 № 259-ФЗ (ред. от 08.08.2024) // Российская газета.
- 2) О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 08.08.2024) // Парламентская газета.
- 3) General Data Protection Regulation (GDPR) // GDPR.EU. URL: <https://gdpr.eu/> (дата обращения: 05.10.2024).
- 4) Loomis J. Algorithmic Due Process: Mistaken Accountability and Attribution in State v. Loomis // Harvard Law Review. 2018. URL: <https://jolt.law.harvard.edu/digest/algorithmic-due-process-mistaken-accountability-and-attribution-in-state-v-loomis> (дата обращения: 23.10.2024).