

Тезисы на тему "Воздействие технологических изменений на юридическую ответственность в области информационного права"

Научный руководитель – Зуева Анна Сергеевна

Алиев Эмин Адилевич

Студент (магистр)

Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра информационной безопасности и компьютерного права, Москва, Россия

E-mail: emin.aliev.2013@list.ru

Современные технологии, такие как искусственный интеллект (ИИ), блокчейн, большие данные, интернет вещей (IoT) и квантовые вычисления, кардинально меняют нашу жизнь. Они открывают новые возможности, но одновременно создают сложные правовые вызовы, особенно в области информационного права. Традиционные правовые нормы, разработанные в эпоху аналоговых технологий, зачастую оказываются неэффективными в условиях цифровой трансформации. Это особенно заметно в вопросах юридической ответственности, где технологии ставят под сомнение привычные подходы к определению вины, причинно-следственных связей и субъектов ответственности. В данной статье рассматриваются ключевые аспекты воздействия технологических изменений на юридическую ответственность в информационном праве и предлагаются пути адаптации правовых норм к новым реалиям.

Искусственный интеллект и автоматизация процессов становятся неотъемлемой частью современного общества. Однако их использование порождает вопросы, связанные с определением субъекта ответственности. Например, если автономная система, управляемая ИИ, причиняет ущерб, кто должен нести ответственность: разработчик, оператор или сама система? В настоящее время правовые системы большинства стран не предусматривают ответственности для ИИ, что создает правовой вакуум.

Примером может служить использование автономных транспортных средств. В случае аварии, вызванной сбоем в работе алгоритма, сложно определить, кто виноват: производитель автомобиля, разработчик программного обеспечения или владелец транспортного средства. Аналогичные вопросы возникают в случаях, когда ИИ генерирует контент, нарушающий авторские права или распространяющий клевету. Для решения этих проблем необходимо разработать четкие правовые рамки, которые учитывали бы специфику ИИ и распределяли ответственность между всеми участниками процесса.

Блокчейн-технологии, лежащие в основе криптовалют и смарт-контрактов, создают новые вызовы для правового регулирования. Одной из ключевых проблем является анонимность участников блокчейн-сетей. Хотя блокчейн обеспечивает прозрачность транзакций, идентификация участников часто затруднена. Это создает сложности при привлечении к ответственности лиц, использующих криптовалюты для незаконных операций, таких как отмывание денег или финансирование терроризма.

Кроме того, смарт-контракты, которые автоматически исполняются при наступлении определенных условий, могут содержать ошибки в коде. Кто должен нести ответственность за ущерб, вызванный такими ошибками: разработчик контракта, платформа или пользователь? Эти вопросы требуют разработки новых правовых норм, которые учитывали бы специфику децентрализованных технологий.

Технологии анализа больших данных позволяют собирать и обрабатывать огромные объемы информации, что создает риски для приватности. Несмотря на существование

законов о защите персональных данных, таких как GDPR в Европе, соблюдение этих норм становится все более сложным в условиях стремительного развития технологий. Утечки данных, вызванные кибератаками или ошибками в системах, становятся все более частыми, что ставит вопрос о распределении ответственности между владельцами данных, операторами и разработчиками.

Примером может служить использование больших данных для микротаргетинга в политической рекламе. Такие практики могут нарушать права граждан на приватность и свободное волеизъявление. Для предотвращения подобных нарушений необходимо ужесточить регулирование и обеспечить прозрачность процессов сбора и использования данных.

Киберпреступность становится одной из главных угроз современного общества. Кибератаки, такие как ransomware-атаки, причиняют значительный ущерб бизнесу и частным лицам. Однако привлечение к ответственности злоумышленников часто затруднено из-за анонимности и трансграничного характера киберпреступлений. Кроме того, возникает вопрос о распределении ответственности между разработчиками, операторами и пользователями в случае уязвимостей в программном обеспечении.

Для борьбы с киберпреступностью необходимо усилить международное сотрудничество и разработать единые стандарты кибербезопасности. Также важно повышать уровень технической грамотности пользователей, чтобы минимизировать риски, связанные с человеческим фактором.

Устройства интернета вещей, такие как умные дома, медицинские устройства и промышленные системы, становятся все более распространенными. Однако их использование создает новые риски для безопасности и приватности. Например, если устройство IoT взломано и используется для незаконных целей, кто должен нести ответственность: производитель, оператор или пользователь?

Кроме того, устройства IoT часто собирают и передают данные без ведома пользователей, что создает риски для приватности. Для решения этих проблем необходимо разработать четкие стандарты безопасности для IoT-устройств и обеспечить прозрачность процессов сбора и использования данных.

Технологические изменения оказывают profound impact на юридическую ответственность в области информационного права. Традиционные правовые нормы зачастую оказываются неэффективными в условиях цифровой трансформации, что требует разработки новых подходов к регулированию. Для решения этих проблем необходимо:

1. Разработать специализированные законы, учитывающие специфику новых технологий.
2. Усилить международное сотрудничество для гармонизации законодательства.
3. Повысить уровень технической грамотности юристов и правоприменителей.
4. Внедрить этические принципы в правовое регулирование технологий.

Только так можно обеспечить баланс между инновациями и защитой прав граждан в условиях стремительного технологического прогресса.

Источники и литература

- 1) 1. Законодательные акты и нормативные документы - Общий регламент по защите данных (GDPR) – Регламент (ЕС) 2016/679. - Федеральный закон "О персональных данных" № 152-ФЗ (Россия). - Директива Европейского парламента и Совета (ЕС) 2019/770 о цифровых услугах и цифровом контенте. - Конвенция о киберпреступности (Будапештская конвенция).
- 2) 2. Научные статьи и монографии - Lessig, L. (1999). *Code and Other Laws of Cyberspace*. Basic Books. - Solum, L. B. (2019). *Artificial Intelligence and the End of

- Law*. SSRN Electronic Journal. - Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs. - Werbach, K. (2018). *The Blockchain and the New Architecture of Trust*. MIT Press.
- 3) 3. Аналитические материалы и отчеты - World Economic Forum (2020). *The Future of Jobs Report*. - McKinsey & Company (2021). *The State of AI in 2021*. - European Union Agency for Cybersecurity (ENISA) (2022). *Threat Landscape Report*. - OECD (2021). *Artificial Intelligence in Society*.
- 4) 4. Статьи и публикации в специализированных изданиях - Calo, R. (2017). *Artificial Intelligence Policy: A Primer and Roadmap*. University of Chicago Law Review. - Casey, A. J., & Niblett, A. (2017). *The Death of Rules and Standards*. Indiana Law Journal. - Finck, M. (2018). *Blockchain Regulation and Governance in Europe*. Cambridge University Press.
- 5) 5. Международные организации и инициативы - Организация Объединенных Наций (ООН) – доклады по вопросам цифровой экономики и кибербезопасности. - Международный союз электросвязи (ITU) – рекомендации по регулированию ИИ и блокчейна. - Европейская комиссия – документы по этике ИИ и регулированию цифровых технологий.