DOI 10.46320/2077-7639-2025-3-136-81-86

Экономико-правовой анализ нелегальных цифровых действий

Баширина Е.Н., Абзгильдин Д.А., Редников Д.В.

Нелегальные цифровые действия охватывают широкий спектр противоправных операций, совершаемых в онлайн-пространстве с целью извлечения материальной выгоды. Цифровая теневая экономика представляет собой сложный социально-экономический феномен, который затрагивает как отдельных пользователей, так и крупные компании, а также государства, включая в себя незарегистрированную торговлю товарами и услугами через интернет, мошенничество с использованием цифровых платежных систем, распространение пиратского контента, организацию кибератак и другие виды нелегальных действий. Объект исследования – цифровая экономика. Предмет исследования – нелегальные цифровые действия. Сделан вывод, что исследование экономико-правовых аспектов нелегальных цифровых действий позволяет получить важные научные и практические результаты, которые способствуют развитию методологии противодействия экономическому преступлению в условиях цифровой эпохи. Данные научные результаты открывают новые перспективы для дальнейших исследований и внедрения инновационных подходов в борьбе с одним из наиболее актуальных вызовов современного общества.

ДЛЯ ЦИТИРОВАНИЯ ГОСТ 7.1–2003

Баширина Е.Н., Абзгильдин Д.А., Редников Д.В. Экономико-правовой анализ нелегальных цифровых действий // Дискуссия. — 2025. — Вып. 136. — С. 81–86.

КЛЮЧЕВЫЕ СЛОВА

Цифровая теневая экономика, цифровая экономика, блокчейн, противоправные действия, мошенничество.

DOI 10.46320/2077-7639-2025-3-136-81-86

An economic and legal analysis of illegal digital activities

Bashirina E.N., Abzgildin D.A., Rednikov D.V.

Illegal digital actions cover a wide range of illegal transactions carried out in the online space for material gain. Digital shadow economy is a complex socio-economic phenomenon that affects both individual users and large companies, as well as states, including unregistered trade in goods and services via the Internet, fraud using digital payment systems, distribution of pirated content, organization of cyberattacks and other types of illegal actions. The object of the study is the digital economy. The subject of the study - illegal digital actions. It is concluded that the study of economic and legal aspects of illegal digital actions allows us to obtain important scientific and practical results that contribute to the development of methodology of countering economic crime in the digital era. These scientific results open new prospects for further research and implementation of innovative approaches in the fight against one of the most pressing challenges of modern society.

FOR CITATION APA

Bashirina E.N., Abzgildin D.A., Rednikov D.V. An economic and legal analysis of illegal digital activities. *Diskussiya [Discussion]*, 136, 81–86.

KEYWORDS

Digital shadow economy, digital economy, blockchain, illegal actions, fraud.

ВВЕДЕНИЕ

Технологические инновации, такие как искусственный интеллект, блокчейн, облачные вычисления и криптовалюты, трансформируют традиционные модели хозяйствования, открывая новые возможности для бизнеса и частных лиц, но наряду с легальными формами использования цифровых технологий активно развиваются и нелегальные действия, которые получили название «цифровая теневая экономика». Особую опасность представляют преступления, совершаемые в «темной сети» (англ. dark web), где злоумышленники могут оставаться анонимными благодаря использованию децентрализованных технологий и шифрования данных. Актуальность темы исследования обусловлена тем, что цифровая теневая экономика становится одним из ключевых факторов, влияющих на развитие современной экономической системы, поэтому ее изучение позволяет не только лучше понять механизмы совершения нелегальных действий, но и разработать эффективные меры их предупреждения и пресечения. Теоретический анализ экономико-правовых аспектов нелегальных цифровых действий является важной научной задачей, решение которой способствует развитию теории и практики противодействия экономическим преступлениям в условиях цифровой трансформации общества. Развитие цифровой теневой экономики создает серьезные вызовы для общества, государства и бизнеса, так как такие действия подрывают доверие к цифровым платформам и технологиям, что замедляет развитие легальной цифровой экономики, но, с другой стороны, они способствуют росту теневого сектора, снижению налоговых поступлений и ухудшению качества государственного управления. Нелегальные цифровые действия могут привести к значительным

финансовым потерям как для частных лиц, так и для компаний, а также создать угрозы для финансовой стабильности на национальном и международном уровнях.

ОСНОВНАЯ ЧАСТЬ

Противодействие масштабированию цифровой теневой экономике требует комплексного научного подхода, включающего совершенствование правовой базы, внедрение передовых технологий защиты данных и повышение осведомленности населения о рисках нелегальной деятельности. В условиях глобализации и трансграничного характера многих преступлений особую важность приобретает международное сотрудничество в сфере кибербезопасности, когда только совместные усилия государства, бизнеса и гражданского общества позволят создать безопасную и надежную цифровую экосистему, которая будет защищать интересы всех участников экономического процесса. Современная эпоха цифровой трансформации экономики характеризуется не только развитием новых форм легальной хозяйственной деятельности, но и активным распространением нелегальных цифровых действий. Эти явления получили название «цифровая теневая экономика», которая охватывает широкий спектр скрытых онлайн-операций, направленных на извлечение материальной выгоды. «*В группе терминов, отражающих природу цифровой теневой деятельности, термин «цифровая теневая экономика» относится к скрытой прибыльной онлайн-торговле или, другими словами, к незарегистрированной прибыльной онлайн-торговле*» [1, с. 176]. Данное определение подчеркивает специфику этого явления, которое включает в себя как нелегальную торговлю товарами и услугами через интернет, так и мошенничество с использованием цифровых платежных систем. Цифровая теневая экономика представляет собой сложный социально-экономический феномен, который затрагивает как индивидуальных пользователей, так и крупные бизнес-структуры, охватывая широкий спектр нелегальных действий, таких как незаконная торговля контрафактными товарами, распространение пиратского контента, мошенничество с использованием криптовалют, а также организацию кибератак и взломов данных. Особую опасность представляют действия, совершаемые в «темной сети», где злоумышленники могут оставаться анонимными благодаря использованию децентрализованных технологий и шифрования данных.

Одним из ключевых факторов, способствующих развитию нелегальных цифровых действий, является наличие правовых пробелов в регулировании цифровой среды. А. Хоффманн, А. Гаспаротти указывают, что существующие правовые механизмы часто оказываются недостаточными для борьбы с нелегальными цифровыми действиями, особенно в контексте международного права [2], что связано с тем, что многие такие действия имеют трансграничный характер, что затрудняет их расследование и привлечение к ответственности. Злоумышленники могут использовать юрисдикционные пробелы для уклонения от ответственности, совершая преступления в одной стране, а получая доход в другой. Недостаточная правовая база в сфере регулирования цифровых платформ создает благоприятную среду для развития нелегальных действий, отсутствие четкого правового статуса криптовалют и блокчейн-технологий усложняет процесс отслеживания транзакций и установления личности участников. А. Хоффманн, А. Гаспаротти подчеркивают необходимость разработки новых правовых механизмов, которые могли бы эффективно противодействовать таким явлениям [2], предлагая внедрить международные стандарты регулирования цифровых платформ, которые позволят унифицировать подходы к борьбе с нелегальной деятельностью на глобальном уровне. Однако разработка новых правовых механизмов сталкивается с рядом сложностей: 1) Высокая скорость технологического прогресса, которая опережает возможности законодательства адаптироваться к новым вызовам; 2) Существует риск нарушения баланса между обеспечением безопасности и защитой прав граждан, таких как право на конфиденциальность и свободу слова. Создание эффективной правовой базы требует тщательного анализа всех аспектов проблемы и учета интересов всех заинтересованных сторон.

Понимание мотивации участников нелегальных цифровых действий является ключевым аспектом их анализа. Согласно зарубежному исследованию Ли Х., основными причинами, побуждающими людей участвовать в таких действиях, являются финансовая выгода, доступность современных технологий и недостаточная эффективность правового регулирования [3]. Например, использование криптовалют позволяет злоумышленникам проводить транзакции анонимно, что затрудняет их отслеживание, как и мотивация злоумышленников.

Важную роль играет психологический аспект: многие участники нелегальных цифровых дей-

ствий воспринимают свои действия как безобидные или даже оправданные, особенно если они считают, что их деятельность не причиняет вреда другим людям. Скачивание пиратского контента часто рассматривается как акт субъективного протеста против завышенных цен на легальные продукты, такое восприятие затрудняет борьбу с нелегальной деятельностью, поскольку оно снижает уровень осознания последствий своих действий среди населения. Одним из наиболее опасных проявлений цифровой теневой экономики является деятельность в «темной сети» (dark web), где злоумышленники могут оставаться анонимными благодаря использованию децентрализованных технологий и шифрования данных. Как отмечается в зарубежном исследовании классификация нелегальных действий в темной сети позволяет выделить несколько ключевых категорий: торговлю наркотиками, оружием, краденными данными, а также организацию кибератак и мошеннических схем [4]. Темная сеть предоставляет уникальные возможности для совершения нелегальных действий, поскольку она позволяет злоумышленникам скрывать свою личность и местоположение, что создает серьезные препятствия для правоохранительных органов, которые сталкиваются с трудностями при выявлении и пресечении таких преступлений. Использование криптовалют в нелегальном секторе интернета затрудняет отслеживание денежных потоков, что делает практически невозможным установление источника доходов преступников. Особую опасность представляют рынки, специализирующиеся на продаже персональных данных, таких как номера банковских карт, пароли и другие конфиденциальные сведения – данные могут быть использованы для совершения мошеннических действий, таких как взлом аккаунтов или хищение средств. В темной сети активно распространяются инструменты для организации кибератак, такие как вредоносное программное обеспечение и эксплойты, что увеличивает масштабы угроз для легальных участников цифровой экономики.

Нелегальные цифровые действия оказывают значительное влияние на экономику, создавая ряд негативных последствий: 1) способствуют росту теневого сектора экономики, что приводит к снижению налоговых поступлений и ухудшению качества государственного управления; 2) такие действия подрывают доверие к цифровым платформам и технологиям, что может замедлить развитие легальной цифровой экономики. И. Е. Милова, А. С. Князькина, А. М. Мозгунова подчеркивают, что нелегальная банковская деятельность, связанная с использованием цифровых технологий, создает серьезные риски для финансовой стабильности [5]. Нелегальные цифровые действия могут привести к значительным финансовым потерям как для частных лиц, так и для компаний, например, мошенничество с использованием фишинговых атак или взломов аккаунтов может привести к утечке конфиденциальной информации и хищению средств.

С экономической точки зрения нелегальная цифровая деятельность создает дисбаланс в конкурентной среде, так как легальные компании вынуждены нести дополнительные расходы на обеспечение кибербезопасности и защиту данных, в то время как нелегальные участники экономики избегают этих затрат, что приводит к искажению рыночных механизмов и снижению эффективности экономической системы в целом. Развитие технологий открывает новые возможности для выявления и противодействия нелегальным цифровым действиям [9]. Одним из перспективных направлений является использование искусственного интеллекта и машинного обучения для анализа больших объемов данных. П. Неруркара предлагает использовать глубокое обучение для обнаружения нелегальных транзакций в криптовалютных сетях [6] – такие технологии позволяют автоматизировать процессы анализа данных и выявления подозрительных паттернов, что значительно повышает эффективность противодействия.

Важную роль играет развитие систем защиты данных и усиление мер кибербезопасности, внедрение многофакторной аутентификации и шифрования данных может значительно снизить вероятность успешных атак на цифровые платформы. Также необходимо развивать системы мониторинга и реагирования на инциденты, которые позволят оперативно выявлять и нейтрализовать угрозы. Особую значимость приобретает использование блокчейн-технологий для отслеживания транзакций и установления их легальности. Блокчейн позволяет создавать прозрачные и неизменяемые записи о всех операциях, что затрудняет скрытие нелегальной деятельности, но для реализации этого потенциала требуется разработка стандартов и протоколов, которые будут поддерживаться всеми участниками цифровой экономики.

Помимо государственных и технологических мер, важную роль в противодействии нелегаль-

ным цифровым действиям играет гражданское общество. Повышение осведомленности населения о рисках цифровой теневой экономики является ключевым фактором, способствующим снижению уровня таких действий. Робертсон К. и др. подчеркивают, что информирование граждан об этических аспектах использования цифровых технологий может способствовать формированию более ответственного отношения к ним [7]. Распространение нелегального контента может быть связано с попытками обойти цензуру или протестными движениями, так как этическая сторона вопроса часто игнорируется участниками нелегальных действий, что создает дополнительные сложности для противодействия таким явлениям [7].

Гражданское общество может сыграть важную роль в формировании общественного мнения и давлении на государство и бизнес для внедрения более эффективных мер противодействия нелегальным цифровым действиям. Например, инициативы по созданию общественных платформ для обмена информацией о киберугрозах могут способствовать более быстрому выявлению и предотвращению преступлений [8].

В ходе исследования эвристически реализуется научно обоснованная классификация нелегальных цифровых действий, учитывающая специфику современных технологий и их использование в преступных целях, основные категории таких действий включают:

I. Финансовые преступления – мошенничество с использованием цифровых платежных систем, незаконный оборот криптовалют, отмывание денег через онлайн-платформы.

II. Киберпреступления, такие как взломы аккаунтов, кража персональных данных, распространение вредоносного программного обеспечения.

III. Нелегальная торговля, продажа контрафактных товаров, наркотиков, оружия и других запрещенных предметов через интернет, особенно в «темной сети» (dark web).

IV. Интеллектуальные права через распространение пиратского контента, нелегальное использование программного обеспечения и медиафайлов.

V. Организация кибератак, проведение DDoS-атак, шпионаж и другие формы вредоносной деятельности.

Данная классификация позволяет систематизировать знания о механизмах совершения преступлений и разрабатывать целевые меры противодействия, адаптированные к каждой категории нелегальных действий.

ЗАКЛЮЧЕНИЕ

Исследование экономико-правовых аспектов нелегальных цифровых действий позволило получить важные научные и практические результаты, которые способствуют развитию методологии противодействия экономическому преступлению в условиях цифровой эпохи. Данные научные результаты открывают новые перспективы для дальнейших исследований и внедрения инновационных подходов в борьбе с одним из наиболее актуальных вызовов современного общества.

Список литературы

1. *Сахбиева, А. И.* Особенности потребительского восприятия «теневого» формата цифровой экономики / А. И. Сахбиева // Modern Economy Success. – 2021. – № 1. – С. 175-179. – EDN QUKRBC.
2. *Хоффман, А., Гаспаротти,* А. Ответственность за незаконный контент в Интернете // Слабые места правовой базы ЕС и возможные планы Комиссии ЕС по их устранению в “Законе о цифровых услугах». – 2020.
3. *Ли, Х.* Обзор мотивов незаконной киберактивности / / Криминология & социальная интеграция: журнал криминологии, пенологии и поведенческих расстройств. – 2017. – Т. 25. – № 1. – С. 110-126.
4. *Хе, С., Хе, Ю., Ли, М.* Классификация незаконной деятельности в даркнете // Материалы 2-й международной конференции по информатике и системам. – 2019. – С. 73-78.
5. *Милова, И. Е., Князькина, А. С., Мозгунова, А. М.* Использование цифровизации при характеристике незаконной банковской деятельности // Современные достижения, вызовы и цифровые возможности экономики, основанной на знаниях. – 2021. – С. 683-691.
6. *Неруркар, П.* Обнаружение незаконной активности в биткойн-транзакциях с помощью глубокого обучения // Программные вычисления. – 2023. – Т. 27. – № 9. – С. 5503-5520.
7. *Робертсон, К. и др.* Незаконное скачивание, этические проблемы и противоправное поведение //Журнал деловой этики. – 2012. – Т. 108. – С. 215-227.
8. *Байниязова,* З. С. Проблема консолидации правового статуса личности в российской правовой системе в цифровую эпоху / З. С. Байниязова, А. В. Бондаренко, М. Ю. Лукиянов // Евразийский юридический журнал. – 2024. – № 1(188). – С. 14-17. – EDN ITCXPS.
9. *Шкляев,* Г. П. Цифровая валюта как средство совершения преступления / Г. П. Шкляев, Н. С. Николаенко, Н. А. Кочоян // Human Progress. – 2024. – Т. 10, № 10. – DOI 10.46320/2073-4506-2024-10a-9. – EDN XMMIEY.

References

1. *Sakhbiyeva, A. I.* Features of consumer perception of the "shadow" format of the digital economy / A. I. Sakhbiyeva // Success of Modern Economy. – 2021. – № 1. – С. 175-179. – EDN QUKRBC.
2. *Hoffmann, A., Gasparotti, A.* Liability for illegal content online // Weaknesses of the EU legal framework and possible plans of the EU Commission to address them in a "Digital Services Act. – 2020.
3. *Li, X.* A review of motivations of illegal cyber activities // Kriminologija & socijalna integracija: časopis za kriminologiju, penologiju i poremećaje u ponašanju. – 2017. – Vol. 25. – № 1. – Pp. 110-126.
4. *He, S., He, Y., Li, M.* Classification of illegal activities on the dark web // Proceedings of the 2nd international conference on information science and systems. – 2019. – Pp. 73-78.
5. *Milova, I. E., Knyaz'kina, A. S., Mozgunova, A. M.* The Use of Digitalization in the Characterization of Illegal Banking Activity // Current Achievements, Challenges and Digital Chances of Knowledge Based Economy. – 2021. – Pp. 683-691.
6. *Nerurkar, P.* Illegal activity detection on bitcoin transaction using deep learning // Soft Computing. – 2023. – Vol. 27. – № 9. – Pp. 5503-5520.
7. *Robertson, K. et al.* Illegal downloading, ethical concern, and illegal behavior //Journal of business ethics. – 2012. – Vol. 108. – Pp. 215-227.
8. *Bainiyazova,* Z. S. The Problem of Consolidating the Legal Status of an Individual in the Russian Legal System in the Digital Age / Z. S. Bainiyazova, A. V. Bondarenko, and M. Yu. Lukiyanov // Eurasian Law Journal. – 2024. – No. 1(188). – Pp. 14-17. – EDN ITCXPS.
9. *Шкляев,* Г. П. Цифровая валюта как средство совершения преступления / Г. П. Шкляев, Н. С. Николаенко, Н. А. Кочоян // Human Progress. – 2024. – Т. 10, № 10. – DOI 10.46320/2073-4506-2024-10a-9. – EDN XMMIEY.

Информация об авторах

Баширина Е.Н., кандидат политических наук, доцент кафедры экономико-правового обеспечения безопасности Института истории и государственного управления Уфимского университета науки и технологий (г. Уфа, Российская Федерация).

Абзгильдин Д.А., старший преподаватель Уфимского университета науки и технологий (г. Уфа, Российская Федерация).

Редников Д.В., старший преподаватель кафедры экономико-правового обеспечения безопасности Института истории и государственного управления Уфимского университета науки и технологий (г. Уфа, Российская Федерация).

Information about the authors

Bashirina E.N., Ph.D. in Politics, Associate Professor of the Department of Economic and Legal Security of the Institute of History and Public Administration of the Ufa University of Science and Technology (Ufa, Russian Federation).

Abzgildin D.A., Senior Lecturer of the Ufa University of Science and Technology (Ufa, Russian Federation). Abramov N.R., Master's student of the Ufa University of Science and Technology (Ufa, Russian Federation).

Rednikov D.V., Senior Lecturer at the Department of Economic and Legal Security Support at the Institute of History and Public Administration of the Ufa University of Science and Technology (Ufa, Russian Federation).