DOI 10.46320/2077-7639-2025-2-135-89-94

Экономическая криминалистика цифрового мошенничества

Баширина Е.Н., Абзгильдин Д.А., Салов И.В., Абрамов И.Р.

Современный этап развития общества характеризуется повсеместной цифровизацией экономических отношений, что воздействует как на механизмы осуществления хозяйственной деятельности, так и методы противодействия преступлениям в экономической сфере. В условиях активного внедрения информационных технологий и расширения сферы их применения, особую актуальность приобретает проблема цифрового мошенничества, которая становится одним из наиболее распространенных видов экономической преступности. Цифровое мошенничество представляет собой сложное социально-экономическое явление, охватывающее широкий спектр противоправных действий, направленных на незаконное извлечение материальной выгоды путем использования современных технологий и манипулирования информацией. Исследование проблематики цифрового мошенничества в рамках экономической криминалистики позволило выявить ряд ключевых результатов, которые имеют как теоретическое, так и практическое значение для противодействия экономическому преступлению в условиях цифровой трансформации общества. Эти результаты базируются на междисциплинарном подходе, объединяющем достижения криминалистики, информационных технологий, права и экономики, и направлены на совершенствование методологии выявления, расследования и предупреждения данного вида преступлений.

ДЛЯ ЦИТИРОВАНИЯ ГОСТ 7.1–2003

Баширина Е.Н., Абзгильдин Д.А., Салов И.В., Абрамов И.Р. Экономическая криминалистика цифрового мошенничества // Дискуссия. — 2025. — Вып. 135. — С. 89–94.

КЛЮЧЕВЫЕ СЛОВА

Цифровой след, цифровое мошенничество, цифровое преступление, экономическая криминалистика, киберпреступление.

DOI 10.46320/2077-7639-2025-2-135-89-94

The economic forensics of digital fraud

Bashirina E.N., Abzgildin D.A., Salov I.V., Abramov I.R.

The modern stage of society development is characterized by the widespread digitalization of economic relations, which affects both the mechanisms of economic activity and methods of counteraction to crimes in the economic sphere. In the conditions of active introduction of information technologies and expansion of their application, the problem of digital fraud, which is becoming one of the most widespread types of economic crime, acquires special relevance. Digital fraud is a complex socio-economic phenomenon, covering a wide range of illegal actions aimed at the illegal extraction of material benefits through the use of modern technologies and manipulation of information. The study of digital fraud within the framework of economic forensics has revealed a number of key results that have both theoretical and practical significance for countering economic crime in the digital transformation of society. These results are based on an interdisciplinary approach that combines the achievements of criminology, information technology, law and economics, and are aimed at improving the methodology of detection, investigation and prevention of this type of crime.

FOR CITATION APA

Bashirina E.N., Abzgildin D.A., Salov I.V., Abramov I.R. The economic forensics of digital fraud. *Diskussiya [Discussion]*, 135, 89–94.

KEYWORDS

Digital footprint, digital fraud, digital crime, economic forensics, cybercrime.

ВВЕДЕНИЕ

Экономическая криминалистика, как научное направление, изучающее закономерности совершения экономических преступлений и разрабатывающая методы их предупреждения, раскрытия и расследования, сталкивается с необходимостью адаптации к новым вызовам цифровой эпохи. Традиционные подходы к анализу преступлений в экономической сфере, основанные на работе с бумажными документами и физическими следами, утрачивают свою эффективность в условиях, когда большинство финансовых операций осуществляется в электронной форме, а следы преступлений остаются в цифровой среде, что требует разработки новых теоретических концепций и практических методик, учитывающих специфику цифровых технологий и особенности функционирования современных информационных систем. Особую сложность представляет тот факт, что цифровое мошенничество отличается высокой степенью латентности, что затрудняет его выявление и учет, так как злоумышленники активно используют анонимность интернет-пространства, децентрализованные системы обмена данными, а также уязвимости программного обеспечения для реализации своих преступных замыслов. При этом масштабы ущерба от таких преступлений постоянно растут, охватывая не только индиви-

дуальных пользователей, но и крупные корпорации, государственные учреждения и даже целые отрасли экономики. Исследование экономической криминалистики цифрового мошенничества представляет собой актуальную научную задачу, решение которой способствует развитию теории и практики противодействия экономическим преступлениям в условиях цифровой трансформации общества. Основными направлениями данного исследования являются анализ методологии выявления и расследования цифровых преступлений, разработка рекомендаций по повышению эффективности правоприменительной практики, а также поиск путей минимизации рисков, связанных с использованием современных технологий в экономической деятельности.

ОСНОВНАЯ ЧАСТЬ

В условиях глобализации и интеграции финансовых рынков последствия цифрового мошенничества могут выходить за национальные границы, создавая дополнительные сложности для правоохранительных органов. Цифровизация экономической деятельности способствует появлению новых форм и методов мошеннических атак, таких как фишинг, социальная инженерия, взломы криптокошельков, использование фальшивых сайтов и мошеннических схем на основе блокчейн-технологий – методы требуют от следственных органов применения специализированных технических средств и аналитических подходов, которые значительно отличаются от традиционных методов расследования. Правовое регулирование цифровых отношений часто отстает от темпов технологического прогресса, что создает правовые пробелы и усложняет процесс привлечения преступников к ответственности. В этих условиях важнейшей задачей экономической криминалистики становится разработка научно обоснованных методов исследования цифровых следов, анализа алгоритмов совершения преступлений и выявления закономерностей поведения злоумышленников в цифровой среде. Это требует междисциплинарного подхода, объединяющего достижения криминалистики, информатики, экономики, юриспруденции и других наук. Особое внимание должно уделяться вопросам совершенствования нормативно-правовой базы, унификации стандартов расследования трансграничных преступлений и разработки механизмов международного сотрудничества в борьбе с цифровым мошенничеством.

В современном мире, в котором финансовые услуги становятся все более доступными благодаря развитию цифровых технологий, растет и количество киберпреступлений, связанных с финансовыми мошенничествами. Цифровые преступления представляют собой сложный феномен, который затрагивает как индивидуальных пользователей, так и крупные бизнес-структуры, но именно индивидуальные пользователи остаются наиболее уязвимой категорией для злоумышленников. «*Основной мишенью финансовых мошенников по-прежнему остаются индивидуальные пользователи финансовых услуг. Подавляющее количество мошеннических атак на индивидуальных пользователей связано с тем, что они, по сравнению с бизнес-структурами, меньше обращают внимание на безопасность и слабо осведомлены о методах мошенничества*» [1, с. 162]. Данное утверждение отечественных исследователей подчеркивает ключевую проблему криминалистики цифрового мошенничества: недостаточная информированность и низкий уровень киберграмотности населения создают благоприятную среду для мошенников, так как в отличие от корпораций, которые часто имеют специализированные службы безопасности, внедряя многоуровневые системы защиты, частные лица зачастую не уделяют должного внимания вопросам кибербезопасности. Это особенно заметно в условиях быстрого развития цифровых технологий, когда новые угрозы появляются быстрее, чем пользователи успевают адаптироваться к ним. Одним из наиболее социально уязвимых направлений финансового мошенничества является использование криптовалют – криптовалюты, такие как биткоин или эфириум, привлекают внимание не только законопослушных участников рынка, но и преступников: «*Преступники используют различные методы для мошенничества с криптовалютами, включая социальную инженерию, взломы, создание фальшивых веб-сайтов и мошеннических схем. Риски включают в себя потерю средств, утечку личных данных, возможные правовые последствия и технические уязвимости криптовалютных систем*» [2, с. 26]. Криптовалюты обладают рядом характеристик, которые делают их привлекательными для мошенников: 1) анонимность транзакций, которая затрудняет отслеживание денежных потоков; 2) децентрализованная природа криптовалют исключает возможность централизованного контроля, что создает дополнительные сложности для правоохранительных органов; 3) многие пользователи, особенно начинающие, не всегда понимают, как правильно хранить свои криптоактивы, что делает их легкой добычей для злоумышленников.

Методы, используемые мошенниками, варьируются от простых до крайне сложных, социальная инженерия, например, основана на манипулировании человеческими эмоциями и доверием. Преступники могут создавать фальшивые сайты, имитирующие популярные платформы для торговли криптовалютами, или отправлять фишинговые письма с целью получения доступа к кошелькам жертв. Взломы также являются распространенным методом, особенно если пользователи используют слабые пароли или не применяют двухфакторную аутентификацию, но даже после совершения преступления задача следственных органов остается чрезвычайно сложной. «*…поисковая деятельность должна осуществляться по определенным логическим правилам, где деятельность следователя по установлению преступника в цифровой среде начинается с анализа уже известных данных – следов, оставленных в цифровой среде и не указывающих на конкретное лицо, совершившее преступление, и продолжается поиском еще не обнаруженных следов, содержащих информацию о лице, совершившем дистанционное мошенничество*» [3, с. 97]. Цифровая среда предоставляет уникальные возможности для сбора данных, но одновременно создает серьезные препятствия для их интерпретации, так как следователи должны анализировать огромные объемы информации, часто разрозненной и запутанной, чтобы выявить улики, которые могут привести к установлению личности преступника. Подобное требует не только глубоких знаний в области информационных технологий, но и владения специализированными инструментами для анализа цифровых следов. Сложность расследования киберпреступлений усугубляется тем, что мошенники постоянно совершенствуют свои методы: «*Мошенничество как разновидность атаки социальной инженерии на рядовых россиян ежедневно совершенствуется с использованием всего арсенала передовых информационных технологий. В целях нивелирования данной проблемы необходимо объединить усилия государства, бизнеса и гражданского общества в борьбе с кибермошенничеством*» [4, с. 80]. Для эффективного противодействия кибермошенничеству требуется комплексный подход, включающий как законодательные меры, так и образовательные программы, где государство должно разрабатывать и внедрять законы, направленные на защиту пользователей цифровых сервисов, а также обеспечивать их исполнение, а бизнес, в свою очередь, обязан внедрять передовые технологии защиты данных и обучать своих клиентов основам кибербезопасности. Гражданское общество может сыграть важную роль, повышая осведомленность населения о рисках и способах защиты от мошенников, но даже при наличии всех этих мер остается одна из самых сложных проблем – правовой статус криптовалют. «*…в настоящее время становится очевидным, что криптовалюта может и выступает в качестве предмета хищений, совершаемых путем обмана и злоупотребления доверием. Однако отсутствие четко законодательно регламентированного правового статуса цифровых валют создает сложности в правоприменении и приводит к неоднородности существующей судебной практики, что в свою очередь может привести к нарушению одного из ключевых принципов уголовного права – восстановления социальной справедливости*» [5, с. 41].

Отсутствие четкого правового регулирования криптовалют создает правовой вакуум, который используется злоумышленниками, в котором судебные органы сталкиваются с трудностями при квалификации преступлений, связанных с криптовалютами, что приводит к неоднородности судебной практики. Например, в одних случаях криптовалюты могут рассматриваться как имущество, в других – как электронные данные – такая неопределенность затрудняет как расследование преступлений, так и восстановление прав потерпевших. Чтобы преодолеть эти сложности, необходимо разработать единый правовой механизм регулирования криптовалют – механизм должен включать в себя четкие определения, правила обращения криптовалют, а также механизмы защиты прав пользователей, обеспечивая международное сотрудничество, поскольку киберпреступления часто имеют трансграничный характер [6]. Финансовые мошенничества в цифровую эпоху представляют собой комплексную проблему, требующую согласованных действий всех заинтересованных сторон. Индивидуальные пользователи, являясь основной мишенью мошенников, нуждаются в повышении уровня киберграмотности. Криптовалюты, будучи новым и быстро развивающимся инструментом, требуют особого внимания как со стороны правоохранительных органов, так и со стороны законодателей. Усиление мер безопасности, развитие технологий расследования и создание единого правового поля станут ключевыми шагами на пути к снижению уровня кибермошенничества и восстановлению социальной справедливости.

В рамках данного исследования объективно установлено, что основные виды цифровых преступлений включают:

— Фишинговые атаки, направленные на получение конфиденциальных данных пользователей (логины, пароли, банковские реквизиты).

— Мошенничество с использованием социальной инженерии, основанное на манипуляции доверием жертв.

— Кражу криптовалют и взломы цифровых кошельков.

— Создание фальшивых сайтов и платформ для незаконного извлечения средств.

— Использование уязвимостей программного обеспечения и блокчейн-технологий.

— Данная классификация позволяет систематизировать знания о механизмах совершения преступлений и разрабатывать целевые меры противодействия.

— Анализ цифровых следов как ключевого элемента расследования.

Исследование показало, что цифровые следы, оставленные злоумышленниками в процессе совершения преступлений, являются основным источником доказательной базы, были выделены следующие категории цифровых следов:

— Технические следы – IP-адреса, метаданные файлов, логи серверов.

— Поведенческие следы, паттерны действий, временные метки, последовательности операций.

— Социальные следы, переписка, публичные сообщения, профили в социальных сетях.

Для эффективного анализа цифровых следов предложено внедрять передовые технологии, такие как искусственный интеллект, машинное обучение и блокчейн-аналитика, которые позволяют автоматизировать процессы сбора и интерпретации данных.

На основе проведенного анализа была разработана комплексная методология расследования цифрового мошенничества, включающая следующие этапы:

1. Идентификация преступления через анализ сигналов о возможном мошенничестве, поступающих от пострадавших, финансовых организаций или автоматизированных систем мониторинга.

2. Сбор и фиксация цифровых доказательств, использование специализированного программного обеспечения для сохранения и анализа данных, полученных из различных источников (электронная почта, социальные сети, блокчейн-транзакции).

3. Реконструкция событий через применение методов цифровой криминалистики для восстановления последовательности действий злоумышленников.

4. Установление личности преступника, использование биометрических данных, анализа IP-адресов и других технических средств для деанонимизации участников преступлений.

5. Правовые и технологические пробелы в противодействии цифровому мошенничеству.

Исследование выявило значительные правовые и технологические пробелы, которые препятствуют эффективному противодействию цифровому мошенничеству достоверно, установлено, что отсутствие четко регламентированного правового статуса криптовалют создает сложности при квалификации преступлений и привлечении злоумышленников к ответственности, возникает необходимость унификации международных стандартов расследования трансграничных преступлений, поскольку большинство цифровых мошенничеств имеет глобальный характер.

Конкретные рекомендации для государственных органов, бизнеса и гражданского общества могут включать в себя следующие элементы:

1. Для государства – это внедрение законодательных норм, регулирующих оборот цифровых активов, усиление контроля за деятельностью криптоплатформ и внедрение механизмов международного сотрудничества в сфере кибербезопасности.

2. Для бизнеса – это развитие систем защиты данных, внедрение многофакторной аутентификации, обучение сотрудников основам киберграмотности и регулярное проведение аудита информационной безопасности.

3. Для гражданского общества – это повышение осведомленности населения о рисках цифрового мошенничества через образовательные программы, кампании по информированию и создание горячих линий для обращений пострадавших.

Ключевые тенденции, по мнению авторов, которые будут определять развитие цифрового мошенничества в ближайшие годы, следующие:

1. Увеличение числа атак на децентрализованные финансовые системы (DeFi) и смарт-контракты.

2. Расширение использования технологий искусственного интеллекта для создания более сложных мошеннических схем.

3. Рост числа трансграничных преступлений, связанных с использованием криптовалют и блокчейн-технологий.

ЗАКЛЮЧЕНИЕ

Полученные результаты исследования имеют высокую научную и практическую значимость. С теоретической точки зрения они расширяют понимание механизмов цифрового мошенничества и методов его противодействия. С практической точки зрения предложенные рекомендации могут быть использованы правоохранительными органами, финансовыми организациями и частными лицами для повышения уровня защиты от киберпреступлений. В конечном итоге, успех в борьбе с финансовыми мошенничествами будет зависеть от того, насколько эффективно государство, бизнес и гражданское общество смогут объединить свои усилия. Только совместная работа государства и заинтересованных сторон позволит создать безопасную и надежную цифровую экосистему, которая будет защищать интересы всех участников финансового рынка.

Список литературы

1. *Котелкин, Ю. В.* Риски финансового мошенничества в условиях цифровой трансформации финансового рынка / Ю. В. Котелкин // Научные труды Северо-Западного института управления РАНХиГС. – 2024. – Т. 15, № 4(66). – С. 161-167. – EDN ALWMMX.
2. *Вестов, Ф. А.* Возможности цифровых технологий по противодействию мошенничеству / Ф. А. Вестов, А. Р. Абдрашитов // Базис. – 2024. – № 2(16). – С. 25-29. – EDN WPQUTN.
3. *Кулаевский, А. В.* Цифровая среда как источник формирования следов лица, совершившего дистанционное мошенничество / А. В. Кулаевский // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. – 2025. – № 25. – С. 96-97. – EDN FKVJAV.
4. *Стрижак, А. Ю.* Зависимость уровня цифрового мошенничества, совершённого с помощью методов социальной инженерии, от экономических факторов в субъектах Российской Федерации / А. Ю. Стрижак, О. А. Пекарская // Экономические и социально-гуманитарные исследования. – 2024. – № 2(42). – С. 68-83. – DOI 10.24151/2409-1073-2024-2-68-83. – EDN ALTXYE.
5. *Перетолчин, А. П.* Цифровая валютакак предмет мошенничества / А. П. Перетолчин // Уголовное право: стратегия развития в XXI веке. – 2024. – № 4. – С. 34-42. – DOI 10.31085/2949-138X-2024-4-328-35-42. – EDN JGFPJB.
6. *Зинченко, Н. Н.* Развитие электронных платежных систем и их влияние на криминогенную обстановку в России / Н. Н. Зинченко // Евразийский юридический журнал. – 2024. – № 10(197). – С. 258-259. – EDN KGGQLW.

References

1. *Kotelkin, Yu. V.* Risks of financial fraud in the conditions of digital transformation of the financial market / Yu. V. Kotelkin // Scientific Proceedings of the North-West Institute of Management of the Russian Academy of National Economy and Public Administration. – 2024. – Vol. 15, № 4(66). – Pp. 161-167. – EDN ALWMMX.
2. *Vestov, F. A.* Opportunities of digital technologies to counteract fraud / F. A. Vestov, A. R. Abdrashitov // Basis. – 2024. – № 2(16). – Pp. 25-29. – EDN WPQUTN.
3. *Kulaevsky, A. V.* Digital environment as a source of formation of traces of the person who committed remote fraud / A. V. Kulaevsky // Actual problems of combating crimes and other offenses. – 2025. – № 25. – Pp. 96-97. – EDN FKVJAV.
4. *Strizhak, A. Yu.* Dependence of the level of digital fraud committed with the help of social engineering methods on economic factors in the subjects of the Russian Federation / A. Yu. Strizhak, O. A. Pekarskaya // Economic and Socio-Humanitarian Studies. – 2024. – № 2(42). – Pp. 68-83. – DOI 10.24151/2409-1073-2024-2-68-83. – EDN ALTXYE.
5. *Peretolchin, A. P.* Digital currency as a subject of fraud / A. P. Peretolchin // Criminal Law: strategy of development in the XXI century. – 2024. – № 4. – Pp. 34-42. – DOI 10.31085/2949-138X-2024-4-328-35-42. – EDN JGFPJB.
6. *Zinchenko,* N. N. The development of electronic payment systems and their impact on the criminal situation in Russia / N. N. Zinchenko // Eurasian Law Journal. – 2024. – № 10(197). – Pp. 258-259. – EDN KGGQLW.

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).

Салов И.В., старший преподаватель кафедры управления информационной безопасностью Института информатики, математики и робототехники Уфимского университета науки и технологий (г. Уфа, Российская Федерация).

Абрамов И.Р., студент Института истории и государственного управления Уфимского университета науки и технологий, независимый исследователь (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).

Salov I.V., Senior Lecturer at the Department of Information Security Management, Institute of Informatics, Mathematics and Robotics, Ufa University of Science and Technology (Ufa, Russian Federation).

Abramov I.R., student of the Institute of History and Public Administration of the Ufa University of Science and Technology, independent researcher (Ufa, Russian Federation)