

ОРГАНИЗАЦИЯ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

DOI: 10.17803/1994-1471.2026.189.8.199-213

Т. Д. Одинокова*,
Ю. В. Шарапов**

Противодействие страховому мошенничеству в условиях цифровизации: новые вызовы для правоохранительных органов и страховых компаний

Аннотация. Страховое мошенничество представляет угрозу для стабильности рыночных отношений, оказывая разрушительное воздействие на операционную эффективность страховых компаний и усугубляя финансовое бремя добросовестных страхователей. Вместе с тем стремительная цифровизация, которая приносит беспрецедентные возможности оптимизации операционных процессов и расширения клиентского сервиса, в то же время радикально трансформирует природу мошеннической деятельности, наделяя злоумышленников принципиально новыми инструментами и каналами для реализации более изощренных, масштабируемых и труднообнаруживаемых схем, таких как манипуляции с цифровыми следами и данными, инсценировки событий с использованием технологий глубокой подделки (deepfake) или эксплуатация уязвимостей в комплексных информационных системах и распределенных реестрах. Это кардинально меняет условия противодействия и, как следствие, формирует новые вызовы для страховых компаний и правоохранительных органов, обуславливая необходимость фундаментальной перестройки их стратегий и тактик. В работе представлены инновационные решения для эффективного противодействия страховому мошенничеству в условиях цифровизации.

Ключевые слова: мошенничество в сфере страхования; мошеннические схемы; незаконные действия; фальсификация; латентность преступления; новые технологии; меры борьбы со страховым мошенничеством; правовое регулирование; сотрудничество; инновации

Для цитирования: Одинокова Т. Д., Шарапов Ю. В. Противодействие страховому мошенничеству в условиях цифровизации: новые вызовы для правоохранительных органов и страховых компаний // Актуальные проблемы российского права. — 2026. — Т. 21. — № 8. — С. 199–213. — DOI: 10.17803/1994-1471.2026.189.8.199-213

© Одинокова Т. Д., Шарапов Ю. В., 2026

* Одинокова Татьяна Дмитриевна, доктор экономических наук, доцент, профессор кафедры бухгалтерского учета и аудита Уральского государственного экономического университета
ул. 8 Марта, д. 62, г. Екатеринбург, Российская Федерация, 620144
tdo17@yandex.ru

** Шарапов Юрий Владимирович, кандидат экономических наук, доцент, доцент кафедры бизнес-информатики Уральского государственного экономического университета
ул. 8 Марта, д. 62, г. Екатеринбург, Российская Федерация, 620144
scharapov_yv@usue.ru

Combating Insurance Fraud in the Age of Digitalization: New Challenges for Law Enforcement and Insurance Companies

Tatyana D. Odinkova, Dr. Sci. (Economics), Associate Professor, Professor, Department of Accounting and Auditing, Ural State University of Economics, Ekaterinburg, Russian Federation
tdo17@yandex.ru

Yury V. Sharapov, Cand. Sci. (Economics), Associate Professor, Associate Professor, Department of Business Informatics, Ural State University of Economics, Ekaterinburg, Russian Federation
scharapov_yv@usue.ru

Abstract. Insurance fraud poses a threat to the stability of market relations, having a devastating impact on the operational efficiency of insurance companies and exacerbating the financial burden on bona fide policyholders. At the same time, rapid digitalization, which brings unprecedented opportunities for optimizing operational processes and expanding customer service, is also radically transforming the nature of fraudulent activity, equipping attackers with fundamentally new tools and channels for implementing more sophisticated, scalable, and difficult-to-detect schemes, such as manipulating digital traces and data, staging events using deepfake technologies, or exploiting vulnerabilities in complex information systems and distributed ledgers. This fundamentally changes the conditions for counteraction and, as a result, creates new challenges for insurance companies and law enforcement agencies, necessitating a fundamental restructuring of their strategies and tactics. The paper presents innovative solutions for effectively combating insurance fraud in the context of digitalization.

Keywords: insurance fraud; fraudulent schemes; illegal actions; falsification; latency of crime; new technologies; measures to combat insurance fraud; legal regulation; cooperation; innovation

Cite as: Odinkova TD, Sharapov YuV. Combating Insurance Fraud in the Age of Digitalization: New Challenges for Law Enforcement and Insurance Companies. *Aktual'nye problemy rossijskogo prava*. 2026;21(8):199-213. (In Russ.). DOI: 10.17803/1994-1471.2026.189.8.199-213

Введение

Страховое мошенничество всегда представляло серьезную проблему для стабильного развития финансового рынка, однако в условиях цифровизации данный феномен приобретает качественно новые масштабы и формы. Стремительное развитие информационных технологий не только расширяет инструментарий мошенников, но и создает принципиально новые схемы обмана, требуя всестороннего пересмотра существующих подходов к его превенции и обнаружению. Согласно отчету CoinLaw «Статистика страхового мошенничества за 2025 год: выявление крупных убытков»¹, мировой объем

страхового мошенничества ежегодно превышает 80 млрд долл. В документе указано, что доля подозрительных выплат по отрасли оценивается в пределах 2–10 % в зависимости от вида бизнеса и юрисдикции, а в некоторых регионах этот показатель достигает 10 %.

Исторически выявление мошенничества во многом зависело от интуиции, опыта и ручного анализа. Однако в условиях экспоненциального роста объемов данных, генерируемых ежедневно, эта традиционная модель больше не является устойчивой. Поэтому, несмотря на многоаспектную изученность проблематики страхового мошенничества, в частности в контексте видо-вого мошенничества², методов его выявления,

¹ Burnett S., Kinder K. Insurance Fraud Detection Statistics 2025: Data-Driven Insights and Detection Techniques // URL: <https://coinlaw.io/insurance-fraud-detection-statistics/> (дата обращения: 20.10.2025).

² Ebinezer M. J. D., Krishna B. C. Life Insurance Fraud Detection: A Data-Driven Approach Utilizing Ensemble Learning, CVAE, and Bi-LSTM // Applied Sciences. 2025. Vol. 15 (16). P. 8869. DOI: 10.3390/app15168869. URL:

предотвращения и привлечения к уголовной ответственности³, а также разработки и применения инструментария для борьбы с ним⁴, тема сохраняет актуальность по ряду причин: динамичное развитие цифровых технологий, усовершенствование моделей взаимодействия на рынке и, соответственно, мошеннических схем, которые создают новые вызовы для страховых компаний и правоохранительных органов, тем самым требуя постоянной адаптации подхода к разработке и внедрению эффективных противодействующих мер, особенно в условиях ускоренной цифровой трансформации всей страховой индустрии.

Именно эта непрерывная эволюция обуславливает научную новизну данного исследования, которая заключается в комплексной систематизации и теоретическом обосновании специфических видов и методов страхового мошенничества, возникающих и трансформирующихся под влиянием цифровизации, а также в разработке адаптивной теоретико-методологической базы для формирования и внедре-

ния инновационных подходов и цифровых инструментов, призванных существенно повысить эффективность систем противодействия злоупотреблениям в страховой сфере в условиях динамично меняющегося технологического ландшафта.

В этой связи целью настоящего исследования является разработка научно обоснованных предложений и практических рекомендаций по совершенствованию системы противодействия страховому мошенничеству, адаптированной к вызовам и возможностям цифровой эпохи, с акцентом на применении передовых информационных технологий для повышения ее превентивного и детектирующего потенциала. Достижение поставленной цели предполагает последовательное решение задач:

1) определить особенности эволюции страхового ландшафта в условиях цифровизации, а также осуществить комплексный анализ современных тенденций и форм страхового мошенничества, детерминированных этим процессом;

<https://www.mdpi.com/2076-3417/15/16/8869> (дата обращения: 30.10.2025) ; *Schalck M. Y.* Auto insurance fraud detection: Leveraging cost sensitive and insensitive algorithms for comprehensive analysis // *Insurance: Mathematics and Economics*. 2025. Vol. 122. P. 44–60. DOI: 10.1016/j.insmatheco.2025.02.001. URL: <https://www.sciencedirect.com/science/article/pii/S0167668725000216> (дата обращения: 26.10.2025) ; *Бердникова О. П., Андроник Н. А.* Отдельные аспекты расследования мошенничества в сфере страхования // *Вестник Уральского юридического института МВД России*. 2019. № 4. С. 57–61.

³ *Kumar S. K., Venkata Gummaadi.* Advancing insurance fraud detection: Leveraging machine learning and AI techniques // *International Research Journal of Modernization in Engineering Technology and Science*. 2024. August. DOI: 10.15680/IJRSET.2024.1308151 ; *Pandya S.* Transforming Claims Processing: The Role of Artificial Intelligence in Enhancing Efficiency and Fraud Detection in the Insurance Industry // *International Journal of Emerging Trends in Computer Science and Information Technology*. 02.07.2025. URL: <https://ijeret.org/index.php/ijeret/article/view/174> ; *Óskarsdóttir M., Ahmed W., Antonio K., et al.* Social Network Analytics for Supervised Fraud Detection in Insurance // *Risk Analysis*. 2021. Vol. 42 (8). DOI: 10.1111/risa.13693 ; *Милова И. Е., Хачатрян Р. Э.* Проблемы привлечения к уголовной ответственности за страховые мошенничества // *Право и государство: теория и практика*. 2025. № 2. С. 597–600. DOI: 10.47643/1815-1337_2025_2_597.

⁴ См.: *Охрименко И. В., Цыганов А. А.* Взгляд практиков: как повысить эффективность противодействия страховому мошенничеству // *Вестник Прикамского социального института*. 2024. № 1 (97). С. 35–39 ; *Они же.* О проблемах противодействия страховому мошенничеству // *Всероссийский криминологический журнал*. 2023. № 5. С. 432–442 ; *Султаниев И. С.* Проблемы противодействия страховому мошенничеству в период цифровой трансформации рынка страховых услуг // *Вестник Московского гуманитарно-экономического института*. 2024. № 3 (95). С. 53–61 ; *Виноходова И. Г.* Методы противодействия мошенничеству в сфере страхования // *Известия Великолукской государственной сельскохозяйственной академии*. 2020. № 1. С. 27–32 ; *Sidorova E.* Current Methods to Combating Insurance Fraud // *Accounting. Analysis. Auditing*. 2024. Vol. 11. P. 93–103. DOI: 10.26794/2408-9303-2024-11-5-93-103.

2) выявить и классифицировать новые и модифицированные виды мошеннических схем, активно использующих цифровые инструменты и платформы, параллельно исследовав специфику законодательного регулирования противодействия страховому мошенничеству;

3) оценить реальные масштабы и структуру страхового мошенничества посредством анализа судебной статистики и экспертных мнений относительно достоверности официальных и неофициальных данных;

4) идентифицировать ключевые вызовы и проблемы, возникающие перед страховыми компаниями и правоохранительными органами в контексте противодействия цифровому страховому мошенничеству;

5) сформировать научно обоснованные практические рекомендации для страховых компаний и правоохранительных органов по адаптации и интеграции цифровых инструментов в комплексную стратегию противодействия страховому мошенничеству.

Результаты

В условиях развития цифровой экономики финансовое мошенничество, в частности в сфере страхования, не просто приобретает новые, более изощренные формы, базирующиеся на передовых цифровых технологиях и искусственном интеллекте (ИИ) для маскировки преступных деяний и увеличения масштабов ущерба, но и становится значимым дестабилизирующим фактором, подрывающим доверие к институтам финансового рынка⁵ и требующим комплексного подхода к разработке и внедрению превентивных мер и механизмов кибербезопасности. В этих условиях, когда цифровые технологии существенно меняют финансовые операции и способы защиты от угроз, становится важным рассмотреть понятие страхового мошенничества как комплекса преднамеренных противо-

правных деяний, осуществляемых отдельными лицами или организованными группами лиц, которые целенаправленно вводят в заблуждение страховую компанию относительно обстоятельств или фактов, имеющих существенное значение, с единственной целью извлечения неправомерной финансовой выгоды.

Субъектный состав данного вида преступности может быть представлен следующими лицами:

1) страхователями, застрахованными, бенефициарами (или выгодоприобретателями);

2) сотрудниками страховой компании, страховыми посредниками, которые либо специализируются на страховании (страховой агент и страховой брокер), либо продают страховые продукты как сопутствующие их финансовым услугам (коммерческие банки, автосалоны, салоны связи, туристические компании и пр.);

3) руководителями и иными высокопоставленными сотрудниками страховой организации.

Идентификация страхового мошенничества базируется на ряде характерных признаков, проявляющихся в различных формах противоправных деяний:

1) предоставлении заведомо ложных сведений, в рамках которого происходит фальсификация информации о наступлении страхового случая, фактически не имеющего места. Например, подача заявления об угоне транспортного средства при отсутствии такового;

2) преувеличении размеров ущерба. Суть этого вида мошенничества заключается в преднамеренном завышении реальной стоимости убытков или объема повреждений после возникновения легитимного страхового случая, что может быть проиллюстрировано некорректным декларированием стоимости поврежденного имущества;

3) инсценировке страховых событий, в рамках которой мошенники целенаправленно создают обстоятельства, имитирующие наступление страхового случая, такой как инсценировка

⁵ Cude B. J., Zhang H. Factors That Influence Willingness to Commit Insurance Fraud // Journal of consumer affairs. 2025. Vol. 59. Iss. 2. P. e70015. DOI: 10.1111/JOCA.70015. URL: <https://onlinelibrary.wiley.com/doi/10.1111/joca.70015> (дата обращения: 06.11.2025).

дорожно-транспортного происшествия или преднамеренный поджог имущества, с целью неправомерного получения страховой выплаты;

4) сокрытии существенной информации, выражающемся в умышленном несообщении страховщику сведений, имеющих существенное значение для оценки страхового риска и определения условий договора. Например, утаивание информации о хронических заболеваниях при оформлении полиса медицинского страхования, что влияет на решение о выдаче полиса или расчет премии;

5) фальсификации документации, заключающейся в использовании поддельных документов, таких как медицинские справки, чеки или акты осмотра, для искусственного подтверждения наступления страхового случая или существенного завышения заявленного размера ущерба.

Законодательное регулирование деликтов в страховой сфере устанавливает правовую основу для квалификации и пресечения страхового мошенничества преимущественно посредством положений УК РФ. Так, статья 159.5 предписывает рассматривать мошенничество с двух позиций, отражающих разные виды противоправных деяний: обман относительно самого факта наступления страхового случая, являющийся ключевым элементом для активации страховых обязательств, и манипуляции с размером страхового возмещения. Данная статья регулирует действия, направленные на получение страховой выплаты путем обмана. Так, если факт мошенничества в страховании выявляется до выплаты возмещения, деяние квалифицируется как покушение на преступление (ст. 30 УК РФ), что влечет более мягкое наказание (ст. 66) по сравнению с оконченным мошенничеством (ст. 159). В некоторых случаях возможно досудебное урегулирование, что позволяет избежать длительного судебного процесса и прекращения дела вне рамок формального разбирательства.

Анализ ст. 159.5 УК РФ показывает, что строгость санкций коррелирует с характером и масштабом деяния, а также с уровнем организованности преступной группы. Изначально за хищение чужого имущества путем обмана относительно наступления страхового случая

могут быть применены такие меры, как штраф до 120 тыс. руб., обязательные или исправительные работы, ограничение свободы, принудительные работы или арест. Однако при наличии квалифицирующих признаков, таких как совершение преступления группой лиц по предварительному сговору, либо лицом с использованием своего служебного положения, либо в крупном размере, а также организованной группой или в особо крупном размере, предусмотрено существенное ужесточение наказания, вплоть до лишения свободы на срок до 10 лет с крупными штрафами и дополнительными ограничениями свободы.

Интересная динамика выявляется при анализе данных: несмотря на значительное повышение эффективности работы с заявлениями о страховом мошенничестве, общее число таких обращений снизилось. В частности, в 2020 г. только 16 % заявлений страховщиков приводили к возбуждению уголовных дел, а к 2024 г. эта доля увеличилась до 34 %, что демонстрирует растущую активность и результативность взаимодействия с правоохранительными органами. Тем не менее количество самих заявлений сократилось с 10 тыс. (на сумму 5,5 млрд руб.) в 2020 г. до 4,5 тыс. (на сумму 3 млрд руб.) в 2024 г.

Экспертные оценки и наблюдения аджастеров — специалистов по урегулированию убытков страховых компаний — свидетельствуют о значительном расхождении между общим количеством выявленных мошеннических деяний в страховой сфере и долей тех из них, которые в конечном итоге доходят до стадии возбуждения уголовного дела или судебного разбирательства, что указывает на проблему латентности преступности и сложности ее юридической квалификации.

Данный феномен находит образное воплощение в концепции айсберга мошенничества в страховании, которая наглядно демонстрирует, что официальная статистика по возбужденным и дошедшим до суда делам представляет собой лишь видимую часть более обширного массива противоправных деяний. Его вершина — это официально зарегистрированные и рассмотренные в суде случаи, тогда как под

водой скрывается основная масса мошеннических попыток, которые либо остаются обнаруженными, либо, будучи выявленными, не получают дальнейшего уголовного преследования. Эта подводная часть включает две основные категории: во-первых, искусно замаскированные мошенничества, которые зачастую не поддаются формальному выявлению и могут быть идентифицированы аджастерами лишь на основе экспертной интуиции, и, во-вторых, случаи мошенничества, которые, будучи обнаруженными, по различным причинам не переходят в стадию уголовного преследования.

Среди превалирующих факторов, обуславливающих значительные сложности в доведении дел о страховом мошенничестве до уголовного преследования, следует особо выделить несколько. Во-первых, это приоритетность задач правоохранительных органов, чья деятельность зачастую ориентирована на расследование более тяжких или резонансных преступлений, что потенциально снижает ресурсы и время, выделяемые на расследование страхового мошенничества. Во-вторых, существенное значение имеет экономическая нецелесообразность для страховых компаний, поскольку издержки, связанные с полноценным уголовным преследованием и сопутствующими судебными процессами, нередко могут превышать потенциальную финансовую выгоду от возмещения ущерба, вынуждая страховщиков прибегать к урегулированию спорных ситуаций на гражданско-правовом уровне. Кроме того, барьером выступает объективная недостаточность доказательств: в процессе расследования часто возникают значительные трудности с формированием неопровержимой доказательной базы, которая соответствовала бы строгим требованиям, предъявляемым к материалам уголовного дела для успешного судебного разбирательства.

Дополнительно стратегический выбор в отношении методов реагирования на страховое мошенничество во многом определяется его

типологией, включающей разделение на «мягкое» и «жесткое». Первое характеризуется преимущественно незначительным завышением или «накручиванием» реальных убытков после фактического наступления страхового случая, что, как правило, не предполагает масштабных преступных схем. В противоположность этому второе представляет собой преднамеренную инсценировку страхового события (например, искусственное создание дорожно-транспортного происшествия, поджог имущества) или фальсификацию ключевых документов, что свидетельствует о более высокой степени криминальной активности и организованности. Именно эта дифференциация видов мошенничества зачастую детерминирует решение страховщика об урегулировании убытков на гражданском уровне, особенно в случаях «мягкого» мошенничества, где трудоемкость и затратность уголовного преследования несоизмеримы с суммой предотвращенного ущерба, что побуждает к менее конфронтационным и более экономически обоснованным внесудебным методам разрешения споров⁶.

Учитывая очерченные выше сложности, связанные с доведением мошеннических деяний до уголовного преследования, а также специфику классификации страхового мошенничества на «мягкое» и «жесткое», можно с очевидностью констатировать обусловленность показателей официальной судебной статистики. Так, анализ удельного веса лиц, обвиняемых по ст. 159.5 УК РФ, в общем показателе обвиняемых за все виды мошенничества за период с 2020 по 2024 г. позволяет оценить динамику и значимость данного вида преступности в структуре общей мошеннической деятельности (рис. 1).

Несмотря на многообразие форм мошенничества, предусмотренных статьями 159–159.6 УК РФ, преступления в сфере страхования составляют лишь около 2 % от общего числа вынесенных приговоров. И. Е. Милова и Р. Э. Хачатрян связывают это с сохраняющейся инерци-

⁶ Insurance Fraud: Impacts on Premiums, Claim Costs, and the Public. Washington : American Academy of Actuaries, 2024. URL: <https://actuary.org/wp-content/uploads/2024/10/casualty-brief-insurance-fraud.pdf> (дата обращения: 27.10.2025).

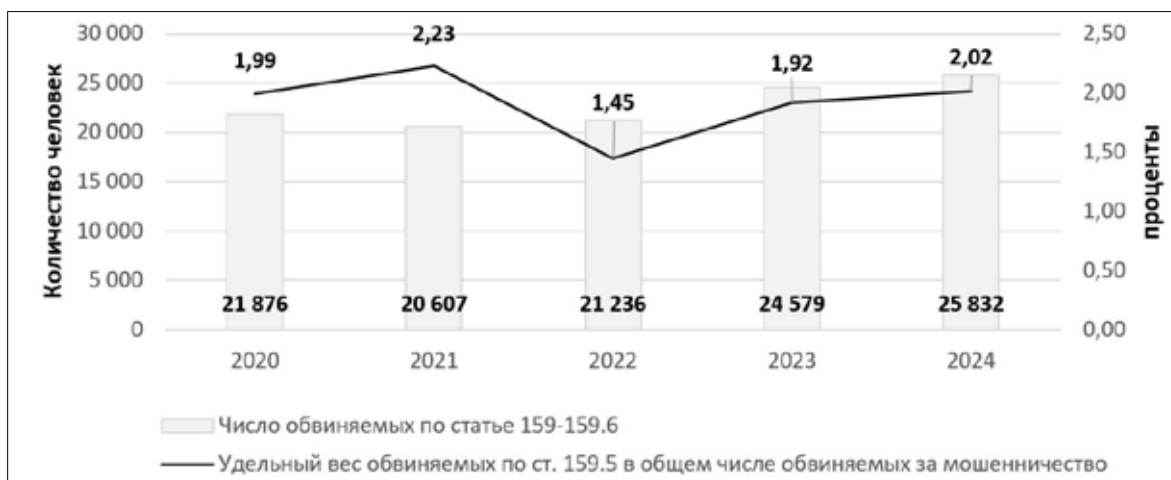


Рис. 1. Удельный вес обвиняемых по ст. 159.5 в общем показателе обвиняемых за все виды мошенничества за 2020–2024 гг., %

ей квалификации по общей статье 159 вместо специальной статьи 159.5 УК РФ, обусловленной коллизиями в юридической конструкции⁷. И. В. Охрименко и А. А. Цыганов, опираясь на мнение экспертного сообщества и результаты исследований, объясняют низкую регистрацию страховых мошенничеств слабостями правоприменения и информационной несогласованностью органов власти и страховых компаний⁸.

На фоне всех перечисленных вызовов и объяснений, касающихся квалификации и выявления, актуальные статистические данные показывают, что в 2024 г. по ст. 159.5 УК РФ обвинялся 521 человек. Однако данный показатель потенциально не отражает в полной мере истинные масштабы рассматриваемой криминальной деятельности ввиду высокой латентности этих правонарушений и сложности их выявления и доказывания, что приводит к систематической недооценке реального ущерба, наносимого страховому рынку, и обуславливает настоятельную потребность в совершенствовании механизмов мониторинга, расследования и судеб-

ного преследования для точного определения масштаба проблемы и разработки эффективных стратегий противодействия.

Несмотря на общую латентность и сложность выявления, даже ограниченный массив данных по вынесенным приговорам предоставляет ценную информацию для понимания внутренней структуры страхового мошенничества: внутри данной категории доминируют две группы деяний. Больше половины обвиняемых по ст. 159.5 УК РФ приходится на случаи, совершенные группой лиц по предварительному сговору или с причинением значительного ущерба (ч. 2 ст. 159.5 УК РФ). Их число выросло втрое с 2016 по 2024 г., достигнув 260 человек. Второе место — около 40 % обвиняемых — занимают особо крупные мошенничества, совершенные организованной группой (ч. 4 ст. 159.5 УК РФ)⁹. Эта категория демонстрирует еще более стремительный рост: количество обвиняемых увеличилось в девять раз за тот же период, составив 213 человек (рис. 2).

⁷ Милова И. Е., Хачатрян Р. Э. Указ. соч. С. 597.

⁸ Охрименко И. В., Цыганов А. А. О проблемах противодействия страховому мошенничеству. С. 434.

⁹ Ковалева Э. Р., Фукина С. П. Страховое мошенничество как фактор, препятствующий развитию страхового рынка России // Азимут научных исследований: экономика и управление. 2019. Т. 8. № 2 (27). С. 161–162.



Рис. 2. Динамика числа обвиняемых по ст. 159.5 УК РФ за 2020–2024 гг.

Подобное усложнение криминальных схем, характеризующееся стремительным ростом числа организованных и групповых мошенничеств, логически вызывает вопрос о характере правовых последствий, применяемых к данным правонарушителям, и об эффективности судебной системы в целом. Анализ распределения приговоров для 521 человека, обвиняемого по ст. 159.5 УК РФ за мошенничество в сфере страхования в 2024 г., представленный на рис. 3, выявляет, что большая часть осужденных (42 %) получили условное наказание. Еще 24 % были приговорены к реальному лишению свободы. Штраф как мера наказания был назначен в 17 % случаев. Менее распространенными видами наказаний стали исправительные (6 %), обязательные работы (3 %) и иные меры (7 %). Примечательно, что за тот же период лишь несколько человек были оправданы по обвинению в страховом мошенничестве.

Эволюция страхового ландшафта, обусловленная интенсивной цифровизацией, создает как существенные преимущества для ведения бизнеса, так и новые векторы потенциального злоупотребления, требующие комплексного подхода к управлению рисками. Ключевыми трендами

цифровизации, трансформирующими страховую отрасль, являются развитие онлайн-каналов продаж (e-commerce), внедрение технологий обработки больших данных (big data), интеграция интернета вещей (Internet of Things, IoT), активное применение ИИ и использование блокчейн-технологий.

Перечисленные тенденции, безусловно, предоставляют страховому бизнесу ряд существенных преимуществ: так, развитие онлайн-продаж не только способствует повышению доступности и удобства услуг для клиентов, но и обеспечивает снижение операционных издержек, возможность персонализации продуктов и значительное ускорение процессов обработки заявлений. Внедрение технологий обработки больших данных и искусственного интеллекта гарантирует продвинутое выявление мошенничества, проактивную идентификацию рисков, оптимизацию ценообразования и существенное ускорение легитимных выплат. Использование интернета вещей способствует представлению объективных доказательств, превентивному предотвращению потерь, активному развитию поведенческого страхования и ускорению урегу-

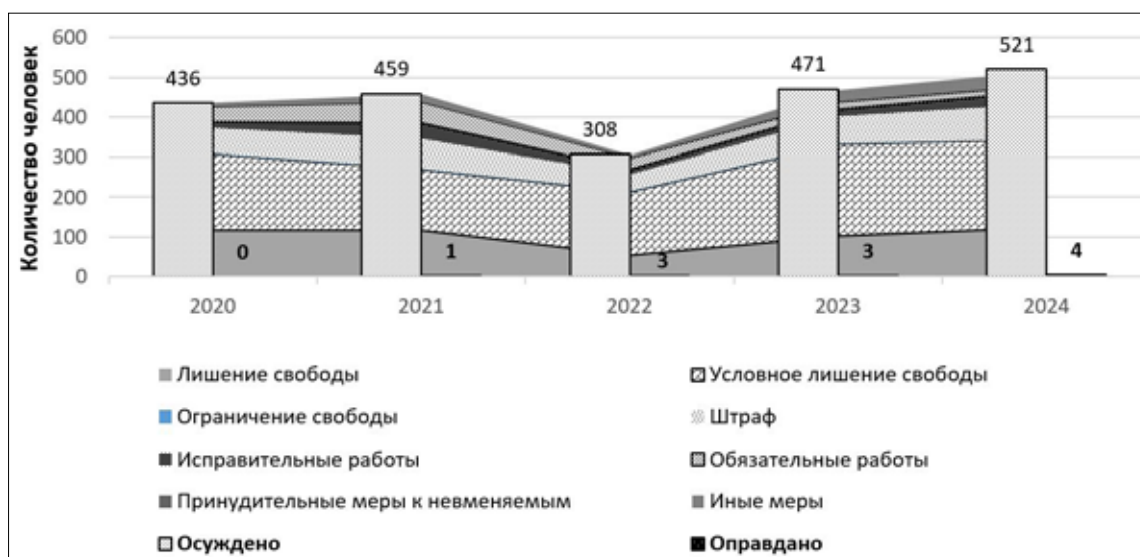


Рис. 3. Динамика числа обвиняемых по мерам наказания за преступления по ст. 159.5 УК РФ за 2020–2024 гг.

лирования убытков, тогда как применение блокчейн-технологий гарантирует неизменяемость и повышает доверие к данным, устраняет необходимость посредников, обеспечивает беспрецедентную прозрачность для всех участников, упрощает верификацию идентичности и активов, а также позволяет осуществлять безопасный и эффективный обмен данными.

Но наряду с преимуществами цифровизация порождает значительный потенциал для злоупотреблений, формируя новые вызовы для страховых компаний и правоохранительных органов. В онлайн-продажах это повышенная анонимность и фейковые данные, ведущие к мошенничеству с платежами и фишингу. Анализ больших данных осложняется маскировкой мошеннических паттернов и созданием синтетических идентичностей. Интернет вещей несет риски манипулирования данными и устройствами, а также риски в сфере кибербезопасности. Искусственный интеллект способствует развитию deepfakes, автоматизации мошеннических схем и обострению «гонки вооружений». Блокчейн-технологии имеют риски, связанные с некорректными входными данными, уязвимостями смарт-контрактов и манипуляциями через «оракулов».

В свете рассмотренных потенциальных угроз страховые компании сталкиваются с рядом вызовов в эффективном противодействии цифровому мошенничеству.

Первый вызов — технологическая «гонка вооружений», обусловленная тем, что мошенники активно используют передовые цифровые технологии (ИИ, глубокое обучение и боты) для создания убедительных фальшивых доказательств, автоматизации мошеннических схем и обхода существующих систем безопасности¹⁰. В связи с этим страховые компании вынуждены постоянно осуществлять инвестиции и обновлять свои антифрод-системы для сохранения превосходства.

Второй вызов — масштаб и сложность анализа больших данных, генерируемых цифровыми системами, поскольку огромные объемы информации, содержащие как ценные паттерны, так и «шум», требуют мощных аналитических инструментов и высококвалифицированных специалистов для выделения релевантных аномалий и интеграции данных из разрозненных источников, что важно для выявления неочевидных связей среди миллионов страховых случаев и заявок.

¹⁰ Schalck M. Y. Op. cit. P. 46.

Третий вызов — верификация цифровых доказательств и их подлинности. С появлением глубокого обучения, сфабрикованных показаний IoT-устройств и онлайн-заявок становится крайне затруднительным подтверждение достоверности предоставляемой информации. При этом традиционные методы проверки демонстрируют неэффективность¹¹, поднимая существенные вопросы о юридической приемлемости и надежности цифровых доказательств в судебных процессах. Примером служит заявление об ущербе, подкрепленное видео, созданным с помощью глубокого обучения, или фальсифицированными данными с автомобильного телематического устройства.

Четвертый вызов — повышенная анонимность и трансграничный характер мошенничества, обусловленные использованием цифровых каналов, VPN и зарубежных серверов, затрудняющие идентификацию и преследование злоумышленников, действующих под чужими или вымышленными именами. Особые сложности возникают при совершении мошенничества из иной юрисдикции, когда группы преступников используют подставные личности и счета из разных стран для подачи множественных заявок через онлайн-формы.

Одновременно правоохранительные органы сталкиваются с уникальными препятствиями при пресечении страхового мошенничества, особенно в цифровой среде. Основными проблемами являются идентификация и юрисдикция преступников, поскольку мошенники используют псевдонимы, анонимные платежные системы (включая криптовалюты) и VPN для сокрытия личности и местоположения, тем самым порождая колоссальные трудности в расследовании трансграничных преступлений.

Существенно осложнены сбор, анализ и верификация цифровых доказательств (из соцсетей, переписки, метаданных, с IoT-устройств), и, как следствие, требуется умение не только извлекать эти данные, но и верифицировать их подлинность (отличить фейки, созданные, например, с использованием ИИ), гарантировать неизменность для судебного процесса и кор-

ректно интерпретировать огромные массивы информации, что предполагает применение специализированных средств цифровой криминалистики.

Продолжая рассмотрение препятствий, отметим технологическую отсталость и дефицит экспертных знаний правоохранительных органов, не обладающих доступом к передовым технологиям и испытывающих нехватку специалистов по кибербезопасности, цифровой криминалистике, анализу больших данных и ИИ, тем самым они оказываются в догоняющей позиции по отношению к мошенникам. Эффективное межведомственное и международное сотрудничество, важное для противодействия трансграничному мошенничеству, затруднено различиями в законодательстве и сложностями обмена конфиденциальной информацией. Существенным вызовом остается несовершенство законодательной базы и регуляторных механизмов, не успевающих за развитием технологий, что приводит к отсутствию четких определений для новых видов мошенничества и адекватных норм об использовании цифровых доказательств. Ограниченные ресурсы и приоритеты правоохранительных органов, а также необходимость соблюдения баланса между приватностью граждан и расследованием при сборе цифровых доказательств, требующая строгого следования законодательству о персональных данных, также являются значимыми препятствиями.

В связи с вышеизложенным цифровизация не просто видоизменяет страховое мошенничество, но и вынуждает правоохранительные органы и страховые компании кардинально менять подходы к его предотвращению и расследованию, превращая эту сферу в постоянную технологическую гонку.

Для эффективного противодействия страховому мошенничеству в России, особенно в условиях развития киберпреступности и новых технологий, необходимо применение комплексного подхода, охватывающего три ключевых направления: совершенствование законодательства, усиление наказаний за кибермошен-

¹¹ Ebinezer M. J. D., Krishna B. C. Op. cit. P. 8869.

ничество в сфере страхования, регулирование использования новых технологий.

Так, по направлению «Совершенствование законодательства» необходимо, во-первых, создать единую информационную базу для эффективного обмена данными¹², что подразумевает разработку и внедрение централизованной высокозащищенной платформы, способной аккумулировать, обрабатывать и стандартизировать предоставлять релевантную информацию о страховых случаях, полисах, участниках инцидентов, а также выявленных прецедентах мошенничества от всех заинтересованных сторон. Предлагаемая интегрированная система призвана преодолеть существующую фрагментацию данных страховых компаний, регулирующих органов, правоохранительных структур и экспертных организаций, затрудняющую выявление и расследование скоординированных мошеннических схем. Используя стандартизированные протоколы обмена и единые форматы данных, платформа обеспечит участникам оперативный доступ к информации для верификации заявлений, идентификации мошеннических паттернов и выявления связей между инцидентами, которые по отдельности могли бы остаться незамеченными. Внедрение такой базы данных ускорит процессы принятия решений, сократит операционные издержки, связанные с ручной обработкой информации, и создаст предпосылки для «масштабируемого... обнаружения мошенничества»¹³ посредством применения передовых аналитических инструментов, включая машинное обучение и искусственный интеллект.

Во-вторых, с целью определения статуса электронных доказательств необходимо, основываясь на принципе недискриминации электронных сообщений¹⁴, разработать и закрепить подход к электронным носителям, цифровым следам, логам транзакций и переписке. В част-

ности, неоднозначность в толковании и применении существующих норм относительно цифровых артефактов часто приводит к их оспариванию оппонентами, затягиванию расследований и даже невозможности привлечения мошенников к ответственности из-за процедурных дефектов в обращении с электронными данными. Для преодоления этих препятствий необходимы законодательные акты, однозначно регламентирующие статус электронных доказательств, их правовой режим, методики извлечения, обеспечения целостности, хеширования, использование электронной подписи и временных меток, а также привлечение квалифицированных экспертов для их анализа. Как следствие, это унифицирует практику применения электронных доказательств, ускорит верификацию и повысит вероятность доказывания мошеннических действий, обеспечивая при этом соблюдение принципов объективности и справедливости в правоприменительной практике¹⁵.

В-третьих, разработать закон «О страховых детективах», что парадоксальным образом сталкивается с выраженным противодействием со стороны государственных правоохранительных структур, их нежеланием делегировать значительную часть полномочий по формированию и верификации доказательственной базы самим страховым организациям.

В рамках первого направления, помимо перечисленного, необходимо усилить международное сотрудничество правоохранительных органов и страховых компаний. Для этого предлагается разработать модельные соглашения об обмене информацией между странами, а также инициировать создание международных рабочих групп по борьбе со страховым мошенничеством, специализирующихся на выявлении и пресечении деятельности организованных

¹² Охрименко И. В., Цыганов А. А. Взгляд практиков... С. 37.

¹³ Ebinezer M. J. D., Krishna B. C. Op. cit. P. 8871.

¹⁴ Афанасьев С. Ф., Борисова В. Ф., Зарубина М. Н. и др. Преимущества и риски применения современных технологий в гражданском процессе // Вестник гражданского процесса. 2020. Т. 10. № 4. С. 281.

¹⁵ Жуйкова А. А. Процессуальные особенности электронных текстовых доказательств как средств доказывания по гражданским делам, связанных с защитой интеллектуальных прав // Актуальные проблемы государства и права. 2020. Т. 4. № 16. С. 536–537. DOI: 10.20310/2587-9340-2020-4-16-530-540.

транснациональных группировок. Использование опыта успешных расследований, осуществленных Интерполом или Европолом, позволит повысить эффективность противодействия трансграничным преступным схемам¹⁶.

По направлению «Усиление наказаний за кибермошенничество в сфере страхования» следует, во-первых, расширить квалифицирующие признаки и отягчающие обстоятельства в ст. 159.5 УК РФ. Действующая редакция, хотя и предусматривает общие квалифицирующие признаки (совершение преступления группой лиц по предварительному сговору, в крупном или особо крупном размере), не всегда адекватно отражает специфику и степень общественной опасности мошеннических действий, реализуемых посредством цифровых инструментов и платформ. Появление новых видов мошенничества, использующих манипуляции с электронными данными, фиктивные цифровые личности, уязвимости систем и элементы искусственного интеллекта, требует детализации законодательства. Включение специфических квалифицирующих признаков, таких как «применение специализированных программных средств», «создание или использование цифровых двойников», «несанкционированное вмешательство в информационные системы» или «массовое распространение ложных сведений посредством цифровых каналов», позволит точнее дифференцировать ответственность.

Аналогично расширение перечня отягчающих обстоятельств, таких как «причинение ущерба, значительно превышающего среднерыночные показатели, посредством эксплуатации цифровых уязвимостей», «трансграничный характер мошенничества», «создание организованной киберпреступной группы» или «неоднократное совершение аналогичных преступлений с использованием идентичных цифровых методов», усилит карательный потенциал нормы. Такая детализация повысит эффективность правоприменения, обеспечит более справедливое наказание и сформирует

предупредительный сигнал для потенциальных правонарушителей.

Во-вторых, необходимо пересмотреть размеры штрафов и сроки лишения свободы, особенно для организованных групп, особо крупных размеров и киберсхем, с целью повышения неотвратимости наказания. Существующие санкции неадекватны современным высокотехнологичным и масштабируемым мошенничествам, в том числе трансграничным; требуется усиление ответственности для организованных преступных формирований с дифференциацией для организаторов.

Что касается мошенничества в особо крупных размерах, текущие штрафы и сроки недостаточны для компенсации ущерба и искупления вины; требуются привязка штрафов к ущербу и увеличение сроков лишения свободы, отражающее масштаб урона экономике и подрыв доверия к страховой системе. Для киберсхем, использующих специфические методы (взлом, фишинг, ИИ) и характеризующихся высокой латентностью и сложностью расследования, необходимы специфические квалифицирующие признаки и ужесточение мер наказания, включая конфискацию специализированного оборудования / ПО и значительное увеличение сроков лишения свободы, что обеспечит неотвратимость наказания и снизит экономическую привлекательность.

В рамках третьего направления «Регулирование использования новых технологий» рекомендуем, во-первых, разработать правовые основы для легитимного применения страховщиками инновационных технологий (ИИ, big data) с целью выявления мошенничества, прогнозирования рисков и анализа аномалий. Без такой регламентации потенциал этих инструментов остается нереализованным из-за существенных юридических рисков и неопределенности в вопросах сбора/обработки чувствительных данных, правомерности автоматизированных решений, ответственности за ошибки алгоритмов и потенциальной дискриминации.

¹⁶ Боровских Р. Н. Типовые механизмы и практика противодействия организованной преступной деятельности в сфере страхования // Lex russica. 2017. № 8 (129). С. 119–134. DOI: 10.17803/1729-5920.2017.129.8.119-135.

Следовательно, специализированная нормативная правовая база, обеспечивающая страховщикам юридически безупречное использование потенциала ИИ и big data, должна гарантировать неукоснительное соблюдение прав граждан на защиту персональных данных, конфиденциальность и недискриминационное отношение. Данная база, включающая регламентацию анонимизации данных, требования к аудиту ИИ-систем, механизмы обжалования автоматизированных решений и этические принципы, максимизирует преимущества технологий и укрепит доверие к страховой системе.

Во-вторых, необходимо ввести специализированные механизмы для технической экспертизы и проверки подлинности цифрового контента. Современные преступные схемы, опираясь на создание и распространение поддельных цифровых артефактов (сфабрикованные фото, видео, документы, аудио), имитирующих реальных людей, затрудняют установление истины. Отсутствие унифицированных и юридически признанных процедур для криминалистического анализа этих материалов создает значительные пробелы при доказывании, требуя комплексного подхода, включающего создание специализированных лабораторий и экспертных центров с передовым программно-аппаратным обеспечением для углубленного анализа и выявления следов редактирования.

Введение указанных механизмов не только значительно повысит эффективность выявления

и расследования мошенничества в сфере страхования, сократит временные и финансовые издержки, но и укрепит принцип неотвратимости наказания, создавая надежный барьер для преступников, стремящихся использовать цифровые технологии для обогащения за счет страховых компаний и добросовестных страхователей.

Заключение

Поскольку страховое мошенничество утрачивает статичность, постоянно трансформируясь под влиянием стремительного развития цифровых технологий и приобретая всё более изощренные, организованные и транснациональные формы, традиционные методы борьбы с ним оказываются недостаточными, что обуславливает острую необходимость комплексного подхода, предполагающего не только интеграцию передовых аналитических систем на основе искусственного интеллекта и машинного обучения для превентивного выявления аномалий и паттернов поведения, но и усиление международного сотрудничества правоохранительных органов и страховых компаний с целью эффективного противодействия трансграничным преступным схемам, а также непрерывное совершенствование нормативной правовой базы для адекватного реагирования на новые вызовы в условиях глобальной цифровизации финансовых рынков.

БИБЛИОГРАФИЯ

1. Афанасьев С. Ф., Борисова В. Ф., Зарубина М. Н. и др. Преимущества и риски применения современных технологий в гражданском процессе // Вестник гражданского процесса. — 2020. — Т. 10. — № 4. — С. 270–294.
2. Бердникова О. П., Андроник Н. А. Отдельные аспекты расследования мошенничества в сфере страхования // Вестник Уральского юридического института МВД России. — 2019. — № 4. — С. 57–61.
3. Боровских Р. Н. Типовые механизмы и практика противодействия организованной преступной деятельности в сфере страхования // Lex russica. — 2017. — № 8 (129). — С. 119–134. — DOI: 10.17803/1729-5920.2017.129.8.119-135.
4. Виноходова И. Г. Методы противодействия мошенничеству в сфере страхования // Известия Великолукской государственной сельскохозяйственной академии. — 2020. — № 1. — С. 27–32. — URL: <https://vgsa.ru/nir/ivgsa/numbers/vgsa2020-1-5.pdf>.
5. Жуйкова А. А. Процессуальные особенности электронных текстовых доказательств как средств доказывания по гражданским делам, связанных с защитой интеллектуальных прав // Актуальные проблемы государства и права. — 2020. — Т. 4. — № 16. — С. 530–540. — DOI: 10.20310/2587-9340-2020-4-16-530-540.

6. Ковалева Э. Р., Фукина С. П. Страхование мошенничества как фактор, препятствующий развитию страхового рынка России // Азимут научных исследований: экономика и управление. — 2019. — Т. 8. — № 2 (27). — С. 160–164.
7. Милова И. Е., Хачатрян Р. Э. Проблемы привлечения к уголовной ответственности за страховые мошенничества // Право и государство: теория и практика. — 2025. — № 2. — С. 597–600. — DOI: 10.47643/1815-1337_2025_2_597.
8. Охрименко И. В., Цыганов А. А. Взгляд практиков: как повысить эффективность противодействия страховому мошенничеству // Вестник Прикамского социального института. — 2024. — № 1 (97). — С. 35–39.
9. Охрименко И. В., Цыганов А. А. О проблемах противодействия страховому мошенничеству // Всероссийский криминологический журнал. — 2023. — № 5. — С. 432–442.
10. Султанов И. С. Проблемы противодействия страховому мошенничеству в период цифровой трансформации рынка страховых услуг // Вестник Московского гуманитарно-экономического института. — 2024. — № 3 (95). — С. 53–61.
11. Burnett S., Kinder K. Insurance Fraud Detection Statistics 2025: Data-Driven Insights and Detection Techniques // URL: <https://coinlaw.io/insurance-fraud-detection-statistics/>.
12. Cude B. J., Zhang H. Factors That Influence Willingness to Commit Insurance Fraud // Journal of consumer affairs. — 2025. — Vol. 59. — Iss. 2. — DOI: 10.1111/JOCA.70015.
13. Ebinezer M. J. D., Krishna B. C. Life Insurance Fraud Detection: A Data-Driven Approach Utilizing Ensemble Learning, CVAE, and Bi-LSTM // Applied Sciences. — 2025. — Vol. 15 (16). — P. 8869–8899. — DOI: 10.3390/app15168869.
14. Insurance Fraud: Impacts on Premiums, Claim Costs, and the Public — Washington : American Academy of Actuaries, 2024. — 11 p. — URL: <https://actuary.org/wp-content/uploads/2024/10/casualty-brief-insurance-fraud.pdf>.
15. Kumar S. K., Venkata Gummadi. Advancing insurance fraud detection: Leveraging machine learning and AI techniques // International Research Journal of Modernization in Engineering Technology and Science. — 2024. — August. — DOI: 10.15680/IJRSET.2024.1308151.
16. Óskarsdóttir M., Ahmed W., Antonio K., et al. Social Network Analytics for Supervised Fraud Detection in Insurance // Risk Analysis. — 2021. — Vol. 42 (8). — DOI: 10.1111/risa.13693.
17. Pandya S. Transforming Claims Processing: The Role of Artificial Intelligence in Enhancing Efficiency and Fraud Detection in the Insurance Industry // International Journal of Emerging Trends in Computer Science and Information Technology. — 02.07.2025. — URL: <https://ijeret.org/index.php/ijeret/article/view/174>.
18. Schalck M. Y. Auto insurance fraud detection: Leveraging cost sensitive and insensitive algorithms for comprehensive analysis // Insurance: Mathematics and Economics. — 2025. — Vol. 122. — P. 44–60. — DOI: 10.1016/j.insmatheco.2025.02.001.
19. Sidorova E. Current Methods to Combating Insurance Fraud // Accounting. Analysis. Auditing. — 2024. — Vol. 11. — P. 93–103. — DOI: 10.26794/2408-9303-2024-11-5-93-103.

Материал поступил в редакцию 6 ноября 2025 г.

REFERENCES (TRANSLITERATION)

1. Afanasev S. F., Borisova V. F., Zarubina M. N. i dr. Preimushchestva i riski primeneniya sovremennykh tekhnologiy v grazhdanskom protsesse // Vestnik grazhdanskogo protsessa. — 2020. — Т. 10. — № 4. — С. 270–294.
2. Berdnikova O. P., Andronik N. A. Otdelnye aspekty rassledovaniya moshennichestva v sfere strakhovaniya // Vestnik Uralskogo yuridicheskogo instituta MVD Rossii. — 2019. — № 4. — С. 57–61.
3. Borovskikh R. N. Tipovye mekhanizmy i praktika protivodeystviya organizovannoy prestupnoy deyatel'nosti v sfere strakhovaniya // Lex russica. — 2017. — № 8 (129). — С. 119–134. — DOI: 10.17803/1729-5920.2017.129.8.119-135.

4. Vinokhodova I. G. Metody protivodeystviya moshennichestvu v sfere strakhovaniya // Izvestiya Velikolukskoy gosudarstvennoy selskokhozyaystvennoy akademii. — 2020. — № 1. — S. 27–32. — URL: <https://vgsa.ru/nir/ivgsa/numbers/vgsa2020-1-5.pdf>.
5. Zhuykova A. A. Protseessualnye osobennosti elektronnykh tekstovykh dokazatelstv kak sredstv dokazyvaniya po grazhdanskim delam, svyazannykh s zashchitoy intellektualnykh prav // Aktualnye problemy gosudarstva i prava. — 2020. — T. 4. — № 16. — S. 530–540. — DOI: 10.20310/2587-9340-2020-4-16-530-540.
6. Kovaleva E. R., Fukina S. P. Strakhovoe moshennichestvo kak faktor, prepyatstvuyushchiy razvitiyu strakhovogo rynka Rossii // Azimut nauchnykh issledovaniy: ekonomika i upravlenie. — 2019. — T. 8. — № 2 (27). — S. 160–164.
7. Milova I. E., Khachatryan R. E. Problemy privilecheniya k ugolovnoy otvetstvennosti za strakhovye moshennichestva // Pravo i gosudarstvo: teoriya i praktika. — 2025. — № 2. — S. 597–600. — DOI: 10.47643/1815-1337_2025_2_597.
8. Okhrimenko I. V., Tsyganov A. A. Vzgl'yad praktikov: kak povysit effektivnost protivodeystviya strakhovomu moshennichestvu // Vestnik Prikamskogo sotsialnogo instituta. — 2024. — № 1 (97). — S. 35–39.
9. Okhrimenko I. V., Tsyganov A. A. O problemakh protivodeystviya strakhovomu moshennichestvu // Vserossiyskiy kriminologicheskij zhurnal. — 2023. — № 5. — S. 432–442.
10. Sultaniev I. S. Problemy protivodeystviya strakhovomu moshennichestvu v period tsifrovoy transformatsii rynka strakhovykh uslug // Vestnik Moskovskogo gumanitarno-ekonomicheskogo instituta. — 2024. — № 3 (95). — S. 53–61.
11. Burnett S., Kinder K. Insurance Fraud Detection Statistics 2025: Data-Driven Insights and Detection Techniques // URL: <https://coinlaw.io/insurance-fraud-detection-statistics/>.
12. Cude B. J., Zhang H. Factors That Influence Willingness to Commit Insurance Fraud // Journal of consumer affairs. — 2025. — Vol. 59. — Iss. 2. — DOI: 10.1111/JOCA.70015.
13. Ebinezer M. J. D., Krishna B. C. Life Insurance Fraud Detection: A Data-Driven Approach Utilizing Ensemble Learning, CVAE, and Bi-LSTM // Applied Sciences. — 2025. — Vol. 15 (16). — P. 8869–8899. — DOI: 10.3390/app15168869.
14. Insurance Fraud: Impacts on Premiums, Claim Costs, and the Public — Washington: American Academy of Actuaries, 2024. — 11 p. — URL: <https://actuary.org/wp-content/uploads/2024/10/casualty-brief-insurance-fraud.pdf>.
15. Kumar S. K., Venkata Gummadi. Advancing insurance fraud detection: Leveraging machine learning and AI techniques // International Research Journal of Modernization in Engineering Technology and Science. — 2024. — August. — DOI: 10.15680/IJRSET.2024.1308151.
16. Óskarsdóttir M., Ahmed W., Antonio K., et al. Social Network Analytics for Supervised Fraud Detection in Insurance // Risk Analysis. — 2021. — Vol. 42 (8). — DOI: 10.1111/risa.13693.
17. Pandya S. Transforming Claims Processing: The Role of Artificial Intelligence in Enhancing Efficiency and Fraud Detection in the Insurance Industry // International Journal of Emerging Trends in Computer Science and Information Technology. — 02.07.2025. — URL: <https://ijeret.org/index.php/ijeret/article/view/174>.
18. Schalck M. Y. Auto insurance fraud detection: Leveraging cost sensitive and insensitive algorithms for comprehensive analysis // Insurance: Mathematics and Economics. — 2025. — Vol. 122. — P. 44–60. — DOI: 10.1016/j.insmatheco.2025.02.001.
19. Sidorova E. Current Methods to Combating Insurance Fraud // Accounting. Analysis. Auditing. — 2024. — Vol. 11. — P. 93–103. — DOI: 10.26794/2408-9303-2024-11-5-93-103.