Научная статья
https://doi.org/10.24412/2220-2404-2025-12-6
УДК 343.98

ОТДЕЛЬНЫЕ ОСОБЕННОСТИ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВ В СФЕРЕ ИНФОБИЗНЕСА

Воротникова А.С.
Юго-Западный государственный университет

Аннотация. *Актуальность настоящего исследования обусловлена стремительной цифровизацией образовательной сферы и сопутствующим ростом экономических преступлений в сфере инфобизнеса. Несмотря на первоначальные попытки правовой регламентации данного рынка, преступления в указанной сфере, продолжают наносить существенный ущерб гражданам и экономической безопасности Российской Федерации. Целью статьи является разработка криминалистических рекомендаций по организации расследования мошенничеств в сфере инфобизнеса. На основе анализа современного состояния рынка рассматриваемого сегмента и резонансных уголовных дел последних лет авторы дают характеристику специфическим элементам информационной модели этих преступлений: способам совершения, обстановке, представляющей собой киберпространство, данным о преступнике, жертве, типичных следах, в том числе цифровых. Научная новизна исследования заключается в адаптации положений частной криминалистической методики к относительно новому и динамично развивающемуся рынку инфобизнеса. В ходе исследования автором сформулированы отдельные криминалистические рекомендации по выявлению и изъятию следов, в том числе цифровых, а также по организации расследования. Предложенные меры направлены на оптимизацию работы следственных органов в целях преодоления противодействия расследованию мошенничеств в сфере инфобизнеса. Практическая значимость работы состоит в повышении эффективности раскрытия и расследования данных видов преступлений.*

Ключевые слова: *экономические преступления, мошенничество, образование, киберпространство, инфобизнес, инфопродукт, криминалистическая характеристика, экономическая безопасность, организованные преступные формирования.*

Финансирование: Работа выполнена в рамках Государственного задания «Правовые меры обеспечения стратегических приоритетов по противодействию угрозам национальной безопасности» (FENM-2025-0010), № 1024031900131-7-5.5.1.

Original article

SPECIFIC FEATURES OF THE INVESTIGATION OF FRAUD IN THE FIELD OF INFORMATION BUSINESS

Anna S. Vorotnikova
Southern State University

Abstract. *The relevance of this study is due to the rapid digitalization of the educational sector and the concomitant increase in economic crimes in the information business. Despite initial attempts at legal regulation of this market, crimes in this area continue to cause significant damage to citizens and economic security of the Russian Federation.The purpose of the article is to develop forensic recommendations for the organization of fraud investigation in the field of information business. Based on the analysis of the current state of the market in this segment and the high-profile criminal cases of recent years, the authors characterize the specific elements of the information model of these crimes: the methods of commission, the cyberspace environment, information about the perpetrator, the victim, and typical traces, including digital ones. The scientific novelty of the research lies in the adaptation of the provisions of private forensic techniques to a relatively new and dynamically developing infobusiness market. In the course of the study, the authors formulated separate forensic recommendations for the identification and removal of traces, including digital ones, as well as the organization of an investigation. The proposed measures are aimed at optimizing the work of investigative authorities in order to overcome the counteraction to the investigation of fraud in the field of information business. The practical significance of the work is to increase the effectiveness of the disclosure and investigation of these types of crimes.*

Keywords: *economic crimes, fraud, education, cyberspace, information business, information product, criminalistic characteristics, economic security, organized criminal formations.*

Funding: The work was carried out within the framework of the State Task "Legal measures to ensure strategic priorities for countering threats to national security" (FENM-2025-0010), № 1024031900131-7-5.5.1.

Введение.

Современный мир представляет собой глобальную и открытую систему знаний, глубокое освоение которых невозможно без научного поиска и самостоятельной деятельности обучающихся. На первый план выходит персонализация обучения, безусловными помощниками которого являются вариативность, деятельностный формат освоения содержимого, проекты, исследования, совместный поиск не только правильных, но и продуктивных решений посредством

сети Интернет. Однако намеченная тенденция на самообучение и саморазвитие в киберпространстве связана с рисками в сфере деятельности недобросовестных участников рынка онлайн-образования, где вопросы вызывает правомерность оказания образовательных услуг, качество реализуемых образовательных программ, не отвечающим соответствующим стандартам и требованиям, квалификация исполнителей.

Деятельность недобросовестных участников рынка онлайн-образования часто связана с извлечением сверхприбыли, что наносит серьезный ущерб как отдельным гражданам, так и государству в целом, и, как следствие, указывает на высокую общественную опасность деяний.

Несмотря на реакцию законодателя в виде внесения изменений и принятия новых нормативных правовых актов, регулирующих порядок реализации образовательных программ с применением электронного обучения и дистанционных образовательных технологий, реализации государственной политики по обеспечению экономической безопасности, ужесточение контроля и надзора за субъектами экономики, экономические преступления в сфере онлайн-образования продолжают наносить весомый ущерб экономике Российской Федерации. Более того, Стратегия экономической безопасности Российской Федерации на период до 2030 года, утвержденная Указом Президента Российской Федерации от 13.05.2017 г. № 208 отмечает развитие современной экономики в условиях, составляющих угрозу для устойчивого роста: недостаточно эффективного государственного управления и сохранения значительной доли теневой экономики.

Результаты.

В настоящем исследовании приведен анализ современного состояния рынка и законодательства онлайн-образования, а также вызовов и рисков указанной сферы. Автор приводит криминалистическую характеристику мошенничества в сфере инфобизнеса на примере резонансных преступлений последних лет, а также формулирует отдельные криминалистические рекомендации по выявлению и изъятию следов, в том числе цифровых, а также организации расследования указанного вида преступлений.

Обсуждение.

В последние годы рынок инфобизнеса стремительно развивается, предоставляя возможность для профессионального роста не только обывателям, но и представителям преступного сообщества. Деятельность по распространению товара или услуги, содержащая специальные знания, удовлетворяющие определенную потребность потребителей, а также направленная на извлечение прибыли от реализации данного информационного продукта (далее по тексту – инфопродукта), получила название инфобизнеса [1, с. 168].

В современном мире выделяют различные формы инфопродуктов: марафоны, курсы, гайды, вебинары, семинары, тренинги, интенсивы и иные [2, с. 32-33].

На данном рынке может быть представлена информация любой направленности: обучающие курсы по иностранным языкам, академическому письму, веб-дизайну, по подготовке к ЕГЭ, бизнес-наставничество и прочее. Потребность в них резко возросла в период пандемии, а затем стала хорошим дополнением к основному и дополнительному образованию при условии законности и добросовестности.

Противоположные примеры связаны обычно с нарушениями авторских и смежных прав, порядка использования персональных данных пользователей, а также случаями мошенничества, уклонения от уплаты налогов, сборов, страховых взносов, легализации денежных средств или иного имущества, приобретенных преступным путем и некоторыми другими.

Оценить доходы от инфобизнеса в полной мере довольно сложно, потому что не всегда субъекты этого рынка декларируют их, образуя, тем самым, теневой сектор экономики. Только по материалам агентства Smart Ranking, во II квартале 2025 года выручка топ-100 крупнейших edtech-компаний составила 34,2 млрд. рублей, в I полугодии 2025 года - 71,6 млрд. рублей, в то время как в 2023 году - 119 млрд. рублей, что на 32% выше 2022 года.

Такие показатели ведущих представителей сегмента онлайн-образования говорят об устойчивом спросе потребителей в этой сфере.

Стоит отметить, что доход инфобизнеса, как и доход от любой другой предпринимательской деятельности, зависит от множества факторов: соотношения цены и качества продукта, уровня конкуренции в нише, маркетинга, квалификации, уровня доверия к продавцу и других. Часто инфобизнес связан с извлечением сверхприбыли, основанной на ажиотажном спросе, порождаемом так называемыми «агрессивными продажами».

Вкупе с ложным завышенным результатом обучения, такие злоупотребления могут повлечь уголовную ответственность, как, например, для бизнес-тренера Аяза Шабутдинова, признанного виновным по делу о мошенничестве в особо крупном размере и приговоренного к семи годам колонии и уплате штрафа в размере 5 млн. рублей.

Криминалистическая характеристика мошенничества в сфере инфобизнеса включает в себя непосредственный предмет преступного посягательства, способ, механизм и обстановку совершения преступного посягательства, типологические черты личности жертвы и преступника [3, с. 330].

Предметом преступного посягательства являются денежные средства, имущество, передаваемые потерпевшим за оказание информационных, образовательных услуг, предоставление доступа к обучающим материалам и т.п.

Среди способов такого мошенничества можно выделить:

- предложение «уникальных» методик быстрого заработка, которые часто являются общедоступной информацией либо не соответствуют заявленным результатам;

- использование социального капитала, фальсификация сведений об опыте работы и квалификации в целях создания ложного положительного представления об обладании преступником специальными знаниями в области предоставляемых услуг;

- использование манипулятивных техник в так называемых «прогревах», включающих методы социальной инженерии, психологическое давление для убеждения потенциальных клиентов в необходимости приобретения инфопродукта;

- создание фиктивных онлайн-школ и платформ с целью сбора денежных средств от клиентов без предоставления качественного обучения или вовсе без предоставления каких-либо услуг.

Чтобы обманным путем завладеть чужими денежными средствами или имуществом под видом предоставления информационных услуг или обучения, преступник следует механизму, включающему в себя несколько этапов.

В ходе подготовительного этапа преступник занимается приисканием соучастников, выбором площадки для преступной деятельности в сети Интернет, созданием «легенды» (позиционирования, личного бренда, уникального товарного предложения), а также анализом целевой аудитории предполагаемых жертв.

Активная реклама и продвижение позволяют охватить большее количество потенциальных клиентов, которые попадут в «воронку продаж» для «прогрева». Ее назначение состоит в том, чтобы вызвать интерес и доверие жертвы для последующей покупки инфопродукта. «Прогрев» представляет собой информационное воздействие на жертву путем манипулятивных техник, убеждения и психологического давления с целью сформировать окончательную готовность совершения покупки инфопродукта.

Совершение преступления включает в себя поступление во владение преступника денежных средств или иного имущества жертвы. Часто, продажа инфопродукта происходит по завышенной цене, не соответствующей его реальной ценности. Обычно, она дифференцируется несколькими тарифами для оплаты с учетом различия в программе обучения.

В целях затруднения отслеживания денежных потоков преступники используют различные платежные системы: электронные кошельки, банковские карты, криптовалюты. Некоторые преступные схемы предполагают вовлечение новых жертв старыми под предлогом предоставления им систем лояльности или иного вознаграждения.

Завершение преступления сопровождается предоставлением доступа к инфопродукту либо без такового. В первом случае, выявляется несоответствие заявленной программы реальному содержанию инфопродукта, низкое качество реализуемых образовательных программ, не отвечающим соответствующим стандартам и требованиям. Преступники перестают выходить на связь, жалобы и требования жертв о возврате денежных средств оставляют без ответа.

В целях сокрытия следов преступления и продолжения аналогичной деятельности, создаются новые аккаунты в социальных сетях, сайты и доменные имена для избежания негативных отзывов и блокировок. Кроме того, преступники переводят полученные деньги на счета, зарегистрированные на третьих лиц или в офшорных зонах, для сокрытия истинного владельца.

Обстановку совершения преступления составляет киберпространство посредством использования сети Интернет с помощью социальных сетей, мессенджеров, сайтов, электронной почты, где, в случае оформления, размещается договор возмездного оказания услуг или оферты, а также организуется коммуникация между жертвой и преступником [4]. Сложности в собирании, изъятии и исследовании цифровых следов затрудняют идентификацию преступника и процесс доказывания, а в условия глобализации и свободного перемещения граждан между государствами, создаются благоприятные возможности, чтобы сокрыться от органов предварительного расследования, а в некоторых случаях - даже анонимности.

Преступниками по делам о мошенничестве в сфере инфобизнеса, как правило, становятся лица, обладающие хорошими навыками общения и убеждения, они используют современные методы маркетинга, рекламы, психологии и информационных технологий, что требует от правоохранительных органов высокого уровня квалификации и технической оснащенности.

Такие преступления часто совершаются организованной группой либо представителями организованных преступных формирований. Если хищение совершено таким образом, то выясняется, когда и при каких обстоятельствах сформировалось преступное формирование, степень его организованности, особенности структуры, связи с аналогичными субъектами, банками и кредитными организациями, властными органами, функции участников, как распределяется похищенное, способы его реализации. Все это предполагает большой объем следственных и оперативно-разыскных действий, использование всего арсенала тактических средств и специальных знаний в области криминалистики, информационных технологий, рынка ценных бумаг, бухгалтерского учета, психологии. Важно выявить лиц с наименее устойчивой мотивацией преступного поведения, чтобы, благодаря им, выяснить криминалистически значимую информацию [5, с. 332].

Жертвами обычно становятся лица, находящиеся в поиске новых возможностей для заработка, повышения квалификации, развития личностного потенциала. Они могут быть подвержены влиянию рекламы и поверить в обещания быстрого успеха. Обычно, это люди со средним или низким уровнем дохода, желающие улучшить свое материальное положение. Опасность мошеннических схем заключается в том, что они ориентированы на широкий круг потенциальных жертв, что позволяет получать значительные доходы даже при небольшом проценте оконченных преступлений.

С учетом этих особенностей, проведение следственных действий имеет специфичный характер. Например, целью допроса подозреваемых, обвиняемых, свидетелей и потерпевших, является не только установление истины по уголовному делу, но и преодоление противодействия расследованию: выявление скрываемой и ложной информации, фактов оказания физического и психологического давления на участников уголовного судопроизводства либо соответствующих угроз, а также шантажа, подкупа, уничтожения или сокрытия следов преступления и прочих способов.

Важная роль при расследовании мошенничеств в сфере инфобизнеса отводится очной ставке, поскольку ее проведение позволяет выявить противоречия в показаниях и установить объективную картину произошедшего.

Проведение обысков и выемок в жилищах, офисах и транспортных средствах участников организованного преступного формирования направлено на выявление и изъятие вещественных доказательств, документов, электронных носителей информации, которые могут подтвердить факт совершения преступлений и участия всех членов организованного преступного формирования.

При расследовании уголовных дел о мошенничестве в инфобизнесе особое внимание следует уделить выявлению и изъятию цифровых следов, что предполагает применение специальных знаний. Цифровые следы по рассматриваемой категории дел могут содержать в себе сведения о транзакциях, геолокации, активности в социальных сетях [6], веб-сайтах, онлайн-платформах и иных площадках, электронную переписку в социальных сетях и мессенджерах, IP-адреса и логи серверов, цифровые документы.

Их изъятие возможно в ходе оперативно-разыскных мероприятий:

- обследования помещений, зданий, сооружений, участков местности и транспортных средств, исследования предметов и документов, снятия информации с технических каналов связи, получения компьютерной информации;

- следственных действий: осмотра места происшествия, предметов и документов, личного обыска, выемки. Однако на практике отмечается «двойственность оформления различными протоколами одного и того же следственного действия».

В связи с этим, мы поддерживаем мнение о необходимости рассмотреть вопрос закрепления осмотра цифровых следов в ч. 1 ст. 144 УПК РФ как «осмотра сетевых информационных ресурсов» [7, с. 102-103].

В уголовных делах о мошенничестве в сфере инфобизнеса при исследовании цифровых следов наиболее целесообразно назначение и проведение судебных психологических, психолого-лингвистических, бухгалтерских, экономических, компьютерно-технических и других экспертиз [8, с. 115-116]. Они позволяют установить роли членов организованного преступного формирования в процессе коммуникации, признаки психологического давления, размер ущерба, выявить способы совершения преступлений, проанализировать финансовые потоки и каналы легализации преступных доходов.

Появление новых форм преступной деятельности было спровоцировано бурным развитием информационных технологий и запоздалой реакцией законодателя вместо опережающего прогноза ситуации и последовательного развития норм, регулирующих образовательную деятельность, защиту прав потребителей, а также предусматривающих ответственность за киберпреступления. Анализ законодательства в сфере онлайн-образования позволяет выявить существующие пробелы, препятствующие эффективной борьбе с мошенничеством в данной сфере.

Важным аспектом является лицензирование и государственная аккредитация образовательной деятельности. Согласно ст. 91 Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», образовательная деятельность подлежит лицензированию. Однако недобросовестные участники рынка инфобизнеса осуществляют свою деятельность в обход этой нормы. Нарушая также Закон РФ от 07.02.1992 № 2300-1 «О защите прав потребителей», они утаивают информацию об образовательной организации и образовательной программе, нарушают право на качественное оказание услуг, на возмещение убытков, причиненных ненадлежащим оказанием услуг, включают в договор условия, ограничивающие ответственность образовательной организации за неисполнение или ненадлежащее исполнение обязательств по договору, а также условия, предусматривающие одностороннее изменение условий договора образовательной организацией.

Несмотря на наличие нормативной правовой базы, регулирующей онлайн-образование и борьбу с киберпреступностью, существуют проблемы, затрудняющие эффективную защиту прав граждан и организаций: отсутствие специализированного законодательства, регулирующего инфобизнес, сложность идентификации лиц, совершающих мошеннические действия в сети «Интернет», недостаточная правовая грамотность потребителей, проблемы выявления, изъятия и исследования цифровых следов в целях доказательства факта оказания образовательных услуг ненадлежащего качества.

Заключение.

Мошенничество в сфере инфобизнеса является серьезной проблемой, требующей комплексного подхода к решению. Действующее законодательство Российской Федерации содержит ряд норм, направленных на пресечение и недопущение таких преступлений, однако существуют пробелы, затрудняющие эффективную защиту прав граждан и организаций.

Для преодоления этих проблем необходимо:

- разработать и принять специализированный закон об инфобизнесе;

- совершенствовать механизмы идентификации лиц, совершающих киберпреступления;

- повышать правовую грамотность потребителей;

- разрабатывать тактические приемы, комбинации, операции по выявлению, изъятию и исследованию цифровых следов, частную криминалистическую методику расследования мошенничества в сфере инфобизнеса и преодоления противодействия со стороны организованных преступных формирований;

- усилить сотрудничество с иностранными государствами в сфере борьбы с киберпреступностью. Реализация этих мер позволит повысить эффективность защиты прав граждан, организаций в сфере инфобизнеса и экономической безопасности страны в целом.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование в формате double-blind peer review (рецензенту неизвестны имя и должность автора, автору неизвестны имя и должность рецензента). Рецензия может быть предоставлена заинтересованным лицам по запросу.

Conflict of Interest

None declared.

Review

All articles are reviewed in the double-blind peer review format (the reviewer does not know the name and position of the author, the author does not know the name and position of the reviewer). The review can be provided to interested persons upon request.

Список источников:

1. Ищук Р.А. Проблемы правового регулирования инфобизнеса: теория и судебная практика // Вопросы российской юстиции. 2025. № 36. С. 166-179. EDN: HJJTYN

2. Кириллова Е. А. Лингвокогнитивные механизмы в продвигающем дискурсе (на примере продажи инфопродуктов блогерами) // Известия Юго-Западного государственного университета. Серия: Лингвистика и педагогика. 2024. Т. 14, № 2. С. 30-41. DOI: 10.21869/2223-151X-2024-14-2-30-41 EDN: FKTOBP

3. Ищенко Е.П. Криминалистика: Курс лекций. - М.: Юридическая фирма "КОНТРАКТ"; АСТ-МОСКВА, 2007. - 416 с.

4. Ефремова И.А., Смушкин А.Б., Донченко А.Г., Матушкин П.А. Киберпространство как новая среда преступности // Вестн. Том. гос. ун-та. 2021. №472. URL: https://cyberleninka.ru/article/n/kiberprostranstvo-kak-novaya-sreda-prestupnosti (дата обращения: 01.11.2025). DOI: 10.17223/15617793/472/29 EDN: ZCBJQG

5. Ищенко Е.П. Криминалистика: Курс лекций. - М.: Юридическая фирма "КОНТРАКТ"; АСТ-МОСКВА, 2007. - 416 с.

6. Кушнарев А.С. Цифровые следы в криминалистике, их использование при расследовании преступлений // Вопросы российской юстиции. 2024. №32. URL: https://cyberleninka.ru/article/n/tsifrovye-sledy-v-kriminalistike-ih-ispolzovanie-pri-rassledovanii-prestupleniy (дата обращения: 10.10.2025). EDN: PDHYXY

7. Назаренко И.С., Митина Е.Н., Меняйло Д.В. О роли и значении цифровых следов и их носителей в рамках процессуальных правоотношений // Судебная экспертиза и исследования. 2025. № 2. С. 99-104. EDN: WUMVBP

8. Отогочев А. В. Виды цифровых следов преступлений на финансовом рынке // Актуальные проблемы российского права. - 2025. - Т. 20. - № 2. - С. 111-124. DOI: 10.17803/1994-1471.2025.171.2.111-124 EDN: LNFMWT

References

1. Ishchuk R.A. Problems of legal regulation of infobusiness: theory and judicial practice // Issues of Russian justice. 2025. No. 36. pp. 166-179. EDN: HJJTYN

2. Kirillova E. A. Linguocognitive mechanisms in the promotional discourse (on the example of the sale of information products by bloggers) // Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Series: Linguistics and Pedagogy. 2024. Vol. 14, No. 2. pp. 30-41. DOI: 10.21869/2223-151X-2024-14-2-30-41 EDN: FKTOBP

3. Ishchenko E.P. Criminalistics: A course of lectures. Moscow: KONTRAKT Law Firm; AST-MOSCOW, 2007. 416 p.

4. Efremova I.A., Smushkin A.B., Donchenko A.G., Matushkin P.A. Cyberspace as a new crime environment // Vestn. Volume of the State University. 2021. No. 472. URL: https://cyberleninka.ru/article/n/kiberprostranstvo-kak-novaya-sreda-prestupnosti (date of request: 11/01/2025). DOI: 10.17223/15617793/472/29 EDN: ZCBJQG

5. Ishchenko E.P. Criminalistics: A course of lectures. Moscow: KONTRAKT Law Firm; AST-MOSCOW, 2007. 416 p.

6. Kushnarev A.S. Digital footprints in criminology, their use in the investigation of crimes // Issues of Russian justice. 2024. No. 32. URL: https://cyberleninka.ru/article/n/tsifrovye-sledy-v-kriminalistike-ih-ispolzovanie-pri-rassledovanii-prestupleniy (date of request: 10.10.2025). EDN: PDHYXY

7. Nazarenko I.S., Mitina E.N., Menyailo D.V. On the role and significance of digital footprints and their carriers in the framework of procedural legal relations // Forensic examination and research. 2025. No. 2. pp. 99-104. EDN: WUMVBP

8. Otogachev A.V. Types of digital traces of crimes in the financial market // Actual problems of Russian law. - 2025. - T. 20. - No. 2. - pp. 111-124. DOI: 10.17803/1994-1471.2025.171.2.111-124 EDN: LNFMWT

Информация об авторе:

Воротникова Анна Сергеевна, преподаватель кафедры уголовного процесса и криминалистики; юридический факультет, Юго-Западный государственный университет; Курск, Россия;. *https://orcid.org/*0000-0002-6438-5478? seamni46@mail.ru

Anna S. Vorotnikova, teacher of the Department of Criminal Procedure and Criminalistics; Faculty of Law, Southwestern State University; Kursk, Russia.

Статья поступила в редакцию / The article was submitted 23.11.2025;
Одобрена после рецензирования / Approved after reviewing 02.12.2025;
Принята к публикации / Accepted for publication 20.12.2025.
Автором окончательный вариант рукописи одобрен.