Научная статья
УДК 343.34

Статья поступила в редакцию 04.04.2025;
одобрена после рецензирования 20.05.2025;
принята к публикации 14.07.2025.

Предпосылки исследования криминальной деятельности участников онлайн-бизнеса

Наталья Анатольевна Логинова, Максим Андреевич Головинский

Санкт-Петербургский университет МВД России, Санкт-Петербург, Россия

Аннотация:
Введение. Ключевой проблемой расследования и предотвращения преступлений в онлайн-бизнесе является недостаток прозрачности всех его сфер деятельности, в т. ч. из-за функционирования в других юрисдикциях. Виртуальные платформы позволяют вести деятельность из других стран и даже в условиях анонимности, что значительно усложняет процесс выявления и идентификации нарушений. Кроме того, онлайн-бизнес часто действует в условиях недостаточной регуляции. Хотя законодательство и адаптируется к новым вызовам цифровой экономики, остаются пробелы в стандартизации и контроле. ***Методы.*** Методологическую основу данного исследования составили общенаучные методы – анализ, синтез, дедукция, индукция и специфические методы – матричный, анкетирования, ранжирования. ***Результаты.*** Выявлены предпосылки исследования криминальной деятельности участников онлайн-бизнеса, что позволило уточнить специфику криминальной деятельности в онлайн-бизнесе по пяти критериям (распространенности; величине ущерба; уровню риска быть пойманным; скорости получения выгоды; количеству участников) и сформулировать задачи и направления развития цифровой криминалистики.

Ключевые слова:
онлайн-бизнес,
криминальная деятельность,
хозяйствующий субъект,
преступления,
цифровая криминалистика

Для цитирования:
Логинова Н. А., Головинский М. А. Предпосылки исследования криминальной деятельности участников онлайн-бизнеса // *Экономическая политика и национальная безопасность*. 2025. № 1 (1). С. 41–52.

Информация об авторах:
Логинова Н. А. – доктор экономических наук, доцент
Санкт-Петербургский университет МВД России
(Российская Федерация, 198206, г. Санкт-Петербург, ул. Летчика Пилютова, д. 1)
профессор кафедры финансового учета и контроля
loginova.79@mail.ru, https://orcid.org/0000-0002-0157-5730
Головинский М. А.
Санкт-Петербургский университет МВД России
(Российская Федерация, 198206, г. Санкт-Петербург, ул. Летчика Пилютова, д. 1)
аспирант кафедры экономической безопасности
maksim.golovinskiy@mail.ru

Original article

The article was submitted April 4, 2025;
approved after reviewing May 20, 2025;
accepted for publication July 14, 2025.

Prerequisites for the research of criminal activities of online business participants

Natalia A. Loginova, Maxim A. Golovinsky

Saint Petersburg University of the MIA of Russia, Saint Petersburg, Russia

Abstract:
Introduction. A key issue in the investigation and prevention of offences in online businesses is the lack of transparency in all areas of their operations, including due to operating in other jurisdictions. Virtual platforms allow activities to be conducted from other countries and even under conditions of anonymity, which significantly complicates the process of detection and identification of offences. In addition, online businesses often operate under a lack of regulation. Although legislation is adapting to the new challenges of the digital economy, standardisation and control gaps remain. ***Methods.*** The methodological basis of this research was formed by general scientific methods – analysis, synthesis, deduction,

induction and specific methods – matrix, questionnaire, and ranking. ***Results.*** The prerequisites for the study of criminal activity of online business participants have been revealed. The authors clarified the specifics of criminal activity in online business according to five criteria (prevalence; magnitude of damage; level of risk of being caught; speed of obtaining benefits; number of participants) and formulated the tasks and directions of development of digital forensics.

Keywords:
online business,
criminal activity,
business entity,
offences,
digital forensics

For citation:
Loginova, Natalia A., and Maxim A. Golovinskiy. 2025. "Predposylki issledovaniya kriminal'noy deyatel'nosti uchastnikov onlayn-biznesa" ["Prerequisites for the research of criminal activities of online business participants"] (In Russ.). *Ekonomicheskaya politika i natsional'naya bezopasnost' [Economic policy and national security]* 1, no. 1 (July): 41–52.

Information about the authors:
Loginova N. A. – Dr. Sci. (Econom.), Docent
Saint Petersburg University of the MIA of Russia (1, Letchika Pilyutova str., Saint Petersburg, 198206, Russian Federation)
Professor of the Department of Financial Accounting and Control
loginova.79@mail.ru, https://orcid.org/0000-0002-0157-5730
Golovinskiy M. A.
Saint Petersburg University of the MIA of Russia (1, Letchika Pilyutova str., Saint Petersburg, 198206, Russian Federation)
Postgraduate student of the Department of Economic Security
maksim.golovinskiy@mail.ru

ВВЕДЕНИЕ

В условиях стремительного развития цифровых технологий и интернет-торговли деловая активность хозяйствующих субъектов возрастает не только в традиционных форматах ведения бизнеса, но появляются и стремительно развиваются принципиально новые его форматы с привлечением сети «Интернет». С каждым годом увеличивается количество платформ и инструментов для ведения онлайн-бизнеса (Власова 2023), что, с одной стороны, расширяет возможности бизнеса, а с другой – делает эту сферу привлекательной для преступников. Криминальные действия в онлайн-среде, такие как мошенничество, отмывание денег и киберпреступность, становятся все более изощренными, а традиционные методы борьбы с ними уже не столь результативны и эффективны.

Сегодня одной из ключевых проблем расследования и предотвращения преступлений в онлайн-бизнесе является недостаток прозрачности всех его сфер деятельности, в т. ч. из-за функционирования в других юрисдикциях. Виртуальные платформы позволяют вести деятельность из других стран и даже в условиях анонимности, что значительно усложняет процесс выявления и идентификации нарушений. Для правоохранительных органов это создает серьезные вызовы, поскольку преступления могут быть скрыты за сложными многоуровневыми схемами, которые трудно отслеживать без специализированных методов анализа и экспертизы. Именно поэтому разработка эффективных инструментов для экономической экспертизы в данной сфере становится крайне необходимой.

Кроме того, онлайн-бизнес часто действует в условиях недостаточной регуляции. Хотя законодательство и адаптируется к новым вызовам цифровой экономики, остаются пробелы в стандартизации и контроле. Комплексное обоснованное исследование криминальных признаков позволит глубже проникнуть в структуру финансовых операций, выявить подозрительные транзакции и схемы, а также предоставит возможность точнее идентифицировать участников преступных действий.

Вместе с тем наряду с трансформацией предпринимательства наблюдается и параллельное развитие криминальной деятельности участников онлайн-бизнеса. В связи с этим возникает необходимость в рассмотрении предпосылок для исследования криминальной активности в сфере онлайн-бизнеса, анализа факторов, способствующих ее возникновению, а также оценки способности правоохранительных органов в выявлении и предотвращении подобных правонарушений.

МАТЕРИАЛЫ И МЕТОДЫ

Существует множество криминологических теорий, дающих представление о причинах совершения противоправных деяний. Рассматривая их в контексте интернет-предпринимательства, можно выделить следующие криминологические концепции: теория дифференциальной ассоциации Эдвина Сатерленда, теория социальной аномии, теория рационального поведения. Систематизируем их положения для целей настоящего исследования.

Теория дифференциальной ассоциации Эдвина Сатерленда. Данная теория была разработана Эдвином Сатерлендом, развита в четвертом издании его труда «Принципы криминологии» (1947) и утверждает, что преступное поведение является результатом социального научения (Sutherland 1947). В соответствии с разработанной Сатерлендом теорией, человек становится преступником не из-за врожденных склонностей, а в результате общения с людьми, которые передают ему ценности, мотивы и методы совершения преступлений. Окружение влияет на восприятие морали и закона, и если большинство людей в среде онлайн-бизнеса считает, что так называемые «серые» и «черные» методы – это нормально, то новый участник начинает воспринимать незаконные действия как обычаи делового оборота (Вакутин 2020).

Таким образом, согласно положениям данной теории, выделим предпосылку криминальной деятельности, характерную в т. ч. и для онлайн-бизнеса.

Предпосылка № 1. Специфические коммуникации между людьми, в рамках которых передаются ценности, мотивы и методы совершения преступлений.

Теория социальной аномии. Концепция Эмилия Дюркгейма и Роберта Мертона объясняет, почему люди совершают преступления. Мертон утверждал, что в обществе есть две неразрывные составляющие – цели и средства. Проблема заключается в том, что не у всех есть равные возможности достичь успеха легальным путем. Когда люди сталкиваются с этим разрывом, возникает аномия – состояние, в котором социальные нормы перестают быть эффективными, и люди выбирают нелегальные способы достижения целей. Кроме того, в современном обществе, особенно в цифровой сфере, популяризируется идея быстрого успеха. В реальности же честный бизнес требует времени, вложений и знаний. Поэтому люди, не имеющие достаточных ресурсов или опыта, ищут обходные пути, попадая в серые и нелегальные схемы (Федотов 2023).

Таким образом, согласно положениям данной теории, выделим следующую предпосылку криминальной деятельности, характерную в т. ч. и для онлайн-бизнеса.

Предпосылка № 2. Популяризация в современном обществе (особенно в цифровой сфере) идеи быстрого (мгновенного) успеха, в то время как в реальной жизни честный бизнес требует существенных затрат времени, вложений и знаний.

Теория рационального поведения. Одна из теорий рационального выбора принадлежит лауреату Нобелевской премии Гэри Беккеру, который разработал экономическую теорию преступления, основанную на принципах рационального выбора. Он считал, что преступники действуют рационально, оценивая выгоды и риски преступления так же, как бизнесмены оценивают инвестиции. На основе данной теории Гэри Беккер вывел формулу ожидаемой полезности совершения преступления (Becker 1968):

$$EU_j = p_j U_j (Y_j - f_j) + (1 - p_j)U_j(Y_j), \quad (1)$$

где: EU_j – ожидаемая полезность индивида j при совершении преступления;
p_j – вероятность быть пойманным и наказанным;
$(1 - p_j)$ – вероятность избежать наказания;
Y_j – доход индивида без совершения преступления;
f_j – размер штрафа / наказания, если преступник будет пойман;
$U_j(Y_j)$ – функция полезности от своего дохода [Becker].

Для иллюстрации данной модели рассмотрим кейс.

Кейс № 1. Предположим, что предприниматель зарабатывает 1 000 000 руб. в год. Если он честно уплатит налог на прибыль как юридическое лицо, то ему придется отдать 200 000 руб. (20 %). Но у него есть возможность скрыть часть доходов и уменьшить налог до 50 000 руб., сэкономив 150 000 руб. Однако если налоговая инспекция обнаружит нарушение, штраф

составит 300 000 руб. Допустим, что вероятность налоговой проверки и выявления нарушения составляет 30 % (p = 0,3). Следовательно, возможны три варианта развития событий:

1 вариант – если предприниматель платит налоги честно, то его доход после уплаты налогов составит 800 000 руб.;

2 вариант – если он уклоняется, и его не ловят, он экономит 150 000 руб., а его доход будет 950 000 руб.;

3 вариант – если он уклоняется и его ловят, то штраф составит 300 000 руб. плюс он обязан выплатить 200 000 руб. в качестве налогов, и итоговый доход составит 500 000 руб.

Таким образом, ожидаемая полезность от уклонения уплаты налога на прибыль с учетом вероятности наказания составит: 1 вариант – 800 000 руб.; 2 вариант – 950 000 руб.; 3 вариант – 500 000 руб.

Теперь сравниваем EU с полезностью честной уплаты налогов U(800 000):

$$EU = 0,3 \times U(500\,000) + 0,7 \times U(950\,000), \quad (2)$$

После вычисления полезности можем сделать один из выводов:

1. Если EU > U(800 000) – уклонение кажется выгодным.

2. Если EU < U(800 000) – лучше заплатить налоги.

Следовательно, штраф или вероятность поимки вырастут, EU_j упадет, и совершение преступления станет менее привлекательным.

Таким образом, согласно положениям данной теории, выделим очередную предпосылку криминальной деятельности, характерную в т. ч. и для онлайн-бизнеса.

Предпосылка № 3. Оценивание преступниками выгод и рисков от результатов совершения преступлений так же, как предприниматели оценивают инвестиционные проекты.

Обобщая вышеизложенное, можно заключить, что одни теории акцентируют внимание на индивидуальных рациональных решениях (как в теории Беккера и теории рационального выбора), другие – на социальных факторах (например, теория дифференциальной ассоциации или теория социальной аномии). Такое разнообразие объясняется сложностью криминального поведения, которое не может быть сведено к одной универсальной модели. В зависимости от контекста преступления (экономическая мотивация, социальное давление, психологические особенности) разные теории могут быть более или менее применимы. Каждая из них акцентирует внимание на определенных аспектах преступности, что позволяет формировать многоуровневые подходы к ее изучению и профилактике. Следовательно, криминологические теории формируют разнообразный аналитический инструментарий, позволяющий изучать преступность с различных точек зрения. Их множественность обусловлена многогранностью факторов, влияющих на преступное поведение.

РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

Вместе с тем современные экономические преступления, совершаемые в цифровой среде, характеризуются высокой степенью анонимности, сложностью финансовых схем и транснациональным характером, что требует применения комплексных экспертных методик (Арженовский и др. 2021).

Экономическая экспертиза позволяет анализировать финансовые потоки, выявлять признаки фиктивного предпринимательства, незаконных транзакций и уклонения от налогообложения. Использование методов судебной бухгалтерии, включающих аудиторский анализ, цифровую криминалистику и идентификацию аномалий в бухгалтерской отчетности, способствует обнаружению схем отмывания денег, финансового мошенничества и манипуляций с активами. В условиях цифровизации экономики данные методы приобретают особое значение, т. к. позволяют проводить комплексный анализ криптовалютных операций, онлайн-платежей, смарт-контрактов и иных финансовых инструментов, используемых в теневом секторе (Филатова и др. 2024). Их интеграция в систему правоохранительных механизмов и регуляторных мер повышает эффективность противодействия преступлениям в сфере электронной коммерции, финансовых технологий и цифровых платформ.

В современном цифровом мире кибермошенничество в финансовой сфере стало одной из наиболее распространенных угроз для бизнеса в целом. Преступники используют фишинг,

вредоносное программное обеспечение и методы социальной инженерии для кражи учетных данных и доступа к банковским счетам хозяйствующих субъектов. Кроме того, взлом систем интернет-банкинга и корпоративных платежных сервисов позволяет злоумышленникам проводить незаконные транзакции и похищать финансовые активы. Не менее серьезной угрозой является подделка электронных платежных документов, что может привести к значительным финансовым потерям и юридическим последствиям для предприятий (Фалина и др. 2023).

В 2024 году на преступления с применением информационно-телекоммуникационных технологий пришлись 40 % всех зарегистрированных в России преступлений[1]. Это наивысший показатель с 2020 года.

В период с января по декабрь 2024 года в России было зафиксировано 765,4 тысячи киберпреступлений, что на 13,1 % больше, чем за аналогичный период 2023 года[2]. Доля киберпреступлений среди всех зарегистрированных преступлений увеличилась с 34,8 % в 2023 году до 40 % в 2024 году[3]. В 2022 году доля IT-преступлений составляла 26,5 % от общего количества преступлений в стране, в 2021 году – 25,8 %, а в 2020 – 25 %[4].

В 2024 году было совершено 84,8 % преступлений с использованием интернета[5] – это четыре из пяти совершенных преступлений. Зарегистрировано 649,1 тысячи таких случаев, что превышает показатели предыдущего года на 23 %[6]. Также в 2024 году возросло число киберпреступлений, связанных со средствами мобильной связи[7]. В 2023 году было зарегистрировано почти 303 тысячи таких случаев, а в 2024 году это число увеличилось на 14,3 % и достигло 346 тысяч[8].

Другим видом преступной деятельности является отмывание денег через цифровые платформы. Преступники активно используют криптовалюты и анонимные платежные системы для сокрытия незаконных доходов, усложняя их отслеживание для финансовых регуляторов. Одним из популярных методов является перевод средств через онлайн-казино, где деньги проходят через многочисленные транзакции, теряя свою первоначальную привязку. Также злоумышленники прибегают к размыванию финансовых потоков с использованием автоматических алгоритмов трейдинга, что делает выявление незаконных схем еще более сложным.

Финансовые пирамиды и инвестиционные мошенничества также приобрели новый облик благодаря цифровым технологиям (Варакса и Бехбудова 2023). Фиктивные инвестиционные платформы, торговые боты и обещания высокой доходности привлекают доверчивых пользователей, которые вкладывают средства в заведомо убыточные схемы. Манипуляции с цифровыми активами, такими как криптовалюты и токены, позволяют мошенникам искусственно завышать их стоимость перед продажей. В результате инвесторы теряют свои вложения, а организаторы схем скрываются.

В 2024 году Банк России выявил 9 027 субъектов (компаний, проектов, индивидуальных предпринимателей и других) с признаками нелегальной деятельности, в т. ч. с признаками финансовых пирамид. Это почти в 1,6 раза больше, чем годом ранее[9].

Статистические данные субъектов финансовых пирамид, собранные Банком России в 2024 году, в сравнении с 2023 годом представлены в таблице 1.

Таким образом, Банк России в 2024 году выявил 5 510 субъектов с признаками финансовой пирамиды. Субъектов с признаками финансовых пирамид выявлено в 1,9 раза больше, чем годом ранее. Увеличилось количество пирамидальных схем с псевдоинвестиционными предложениями, которые публично привлекают средства в сомнительные проекты, обещая гарантированный доход.

---

[1] В России в 2024 году IT-преступления достигли пика за последние 5 лет // *Информационное телеграфное агентство России (ИТАР-ТАСС)* : [сайт]. URL: https://tass.ru/proisshestviya/22978955 (дата обращения: 30.04.2025).

[2] Там же.

[3] Там же.

[4] Там же.

[5] Там же.

[6] URL: https://tass.ru/proisshestviya/22978955 (дата обращения: 30.04.2025).

[7] Там же.

[8] Там же.

[9] Противодействие нелегальной деятельности на финансовом рынке // *Банк России* : [официальный сайт]. URL: https://cbr.ru/analytics/inside/2024_2/ (дата обращения: 05.03.2025).

Таблица 1

Субъекты с признаками финансовой пирамиды

Table 1

Entities with signs of a pyramid scheme

Субъекты	2023 год	2024 год
Интернет-проекты	2 886	5 457
Общества с ограниченной ответственностью	15	16
Потребительские кооперативы	16	4
Иные формы	27	33
Всего выявлено	2 944	5 510

Источник: разработано авторами на основании данных Банка России[10].

Классические пирамиды сохранились, и даже вернулась практика проводить презентации, обзванивать потенциальных клиентов, приглашать их в офис (Авагян и др. 2024). Однако самыми популярными остаются схемы с упоминанием криптовалют. Причем их организаторы действуют не только в интернете, но и офлайн[11]. Помимо предложений инвестировать в перспективные криптопроекты, мошенники используют криптовалюту, чтобы привлекать средства. В 2023 году взносы в криптовалютах принимали 50 % пирамидальных проектов, в 2024 году – 77 %[12]. В то же время снизилась популярность пирамидальных схем в форме экономических игр с псевдоинвестиционной составляющей: в 2023 году было выявлено 529 таких нелегальных проектов, в 2024 году – 379[13].

Почти 20 % проектов с признаками финансовых пирамид имели более двух интернет-ресурсов[14]. Сайты и страницы в соцсетях создаются массово, с шаблонным оформлением, меняются только названия используемых брендов и компаний. Для привлечения клиентов также активно используются телеграм-каналы: в 2024 году было выявлено более 1 300 таких ресурсов, в 2023 году — 1 200[15]. Использование для раскрутки проектов страниц в соцсетях стало менее популярным: 690 страниц было выявлено в 2024 году, 1 200 — в 2023 году[16].

В 2024 году по результатам рассмотрения материалов, направленных регулятором (в т. ч. за предыдущие периоды), были приняты следующие меры: возбуждено более 650 административных дел по различным статьям Кодекса Российской Федерации об административных правонарушениях[17] (в т. ч. более 500 дел по статье за незаконное осуществление профессиональной деятельности по предоставлению потребительских займов); принято более 1 180 иных мер реагирования; ограничен доступ более чем к 17 тыс. ресурсов в сети «Интернет», которые принадлежали нелегальным участникам финансового рынка и субъектам с признаками финансовых пирамид[18].

По договоренности с Банком России хозяйствующие субъекты, работающие на рынке антивирусного программного обеспечения, добавляют в свои базы данные о подобных ресурсах, чтобы снизить риски перехода на подозрительные сайты.

---

[10] Список компаний с выявленными признаками нелегальной деятельности на финансовом рынке // *Банк России* : [официальный сайт]. URL: https://cbr.ru/inside/warning-list/ (дата обращения: 05.03.2025).

[11] Плугатырева Д. А., Чурилова А. А. Финансовые пирамиды как один из видов финансового мошенничества // *Современные научные взгляды в эпоху глобальных трансформаций: проблемы, новые векторы развития* : материалы XLII Всероссийской научно-практической конференции, г. Ростов-на-Дону, 16 декабря 2021 г. Ростов-на-Дону : Издательство ВВМ, 2021. С. 1077–1078.

[12] URL: https://cbr.ru/inside/warning-list/ (дата обращения: 05.03.2025).

[13] Там же.

[14] Там же.

[15] Там же.

[16] Там же.

[17] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (ред. от 07.04.2025) // *Собрание законодательства Российской Федерации*. 2002. № 1 (ч. 1). Ст. 1.

[18] URL: https://cbr.ru/inside/warning-list/ (дата обращения: 05.03.2025).

Не менее опасными являются налоговые преступления с применением цифровых технологий[19]. Современные офшорные схемы включают использование криптовалют для сокрытия доходов и обхода налогового законодательства. Некоторые хозяйствующие субъекты искусственно занижают налогооблагаемую базу с помощью цифровой бухгалтерии, подделки отчетности и использования сложных финансовых манипуляций (Есаков и Саушкин 2020). В последние годы особую роль в уклонении от налогов играет автоматизация процессов с применением искусственного интеллекта, который анализирует налоговые лазейки и помогает обходить финансовые регуляции.

Количество выявленных налоговых преступлений неуклонно растет (см. таблицу 2).

Таблица 2

Динамика количества налоговых преступлений с применением цифровых технологий

Table 2

Dynamics of the number of digital tax offences

Выявлено	Год											
	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Количество преступлений	1 655	1 831	2 022	3 111	2 428	2 894	2 798	2 675	2 896	3 458	4 117	5 230

Источник: *составлено авторами.*

Анализ данных таблицы 2 позволяет заключить, что за период с 2013 по 2024 гг. произошел более чем трехкратный рост налоговых преступлений с применением цифровых технологий, что обусловлено следующими причинами: стремительное развитие цифровых технологий (расширение использования электронных «наличных», электронной торговли, технологии блокчейна, цепочек поставок, одноранговых сетей и пр.); усиление налоговой нагрузки; сокращение наличных расчетов; упрощение перевода прибыли с помощью трансфертного ценообразования; размещение нематериальных активов в юрисдикциях с низким налогообложением; перераспределение корпоративного долга; заключение отвлекающих договоров, корпоративных инверсий и пр.

Одним из наиболее сложных для расследования преступлений в цифровой среде остается корпоративный шпионаж и утечка данных (Воротникова 2024). Злоумышленники взламывают корпоративные базы данных для получения конфиденциальной информации, включая коммерческие тайны и пользовательскую информацию. Кроме того, инсайдерская информация используется для манипуляций на фондовых рынках, позволяя нечестным игрокам зарабатывать на предсказуемых изменениях котировок. Современные технологии, такие как *Deepfake*, также применяются для подделки цифровых документов и компрометации ключевых фигур в бизнесе, создавая угрозу не только для финансовых активов, но и для репутации компаний (Воловик 2024).

В 2024 году более половины (52 %) успешных атак на организации закончились утечкой данных[20]. Наиболее часто жертвами утечек становились государственные учреждения (13 %), промышленность (10 %), *IT*-компании (10 %), финансовые организации (8 %) и медицинские учреждения (7 %)[21].

Применение цифровых технологий в вопросе совершения экономических преступлений может происходить в следующих формах: фишинг, хакинг, криптоджекинг, спуфинг,

[19] Тороп С. С. Тенденция развития криминогенной обстановки совершения налоговых преступлений в современной России: понятие и особенности расследования налоговых преступлений // *Устойчивое развитие в неустойчивом мире* : сборник научных статей Международной научно-практической конференции, г. Самара, 23 мая 2023 г. Самара : Самарский государственный экономический университет, 2023. С. 153–164. https://doi.org/10.46554/UR-2023-pp.153.

[20] Утечки конфиденциальных данных организаций в 2024 году // *Positive Technologies* : [сайт]. URL: https://ptsecurity.com/ru-ru/research/analytics/utechki-dannyh-aktualnye-ugrozy-vtorogo-polugodiya-2024-dlya-organizaczij/#id21 (дата обращения: 30.04.2025).

[21] Там же.

программы-вымогатели; межсайтовый скриптинг, «кража личности», «социальная инженерия», *DDoS*-атаки, *Black Hat SEO*.

1. Фишинг – обман пользователей с целью получения конфиденциальных данных.

2. Хакинг – взлом систем для кражи информации.

3. Криптоджекинг – незаконное использование вычислительных мощностей для добычи (майнинга) криптовалюты.

4. Спуфинг – подмена информации для обмана пользователей.

5. Программы-вымогатели – блокировка данных с требованием выкупа.

6. Межсайтовый скриптинг – внедрение вредоносного кода на сайты.

7. «Кража личности» – незаконное использование персональных данных для получения материальной выгоды.

8. «Социальная инженерия» – психологическое воздействие на человека с целью совершения им определенных действий.

9. *DDoS*-атаки – парализация работы компаний через массовые запросы к серверам.

10. *Black Hat SEO* – использование запрещенных приемов для целей продвижения сайта в результатах поисковых запросов.

С целью уточнить специфику криминальной деятельности в онлайн-бизнесе нами было проведено анкетирование, в рамках которого респондентам предлагалось проранжировать рассмотренные формы экономических преступлений применительно к онлайн-бизнесу по нескольким критериям:

1) по распространенности;

2) по величине ущерба;

3) по уровню риска быть пойманным;

4) по скорости получения выгоды;

5) по количеству участников.

Максимальное значение ранга соответствует большему (лучшему) значению, минимальное значение ранга – меньшему (худшему) значению. Анкета была размещена на платформе *Google* с 10 января года по 1 апреля 2025 г. Всего в опросе приняли участие – 369 респондентов (представители бизнеса и правоохранительных органов).

На основании данных, представленных в таблице 3, можно сделать следующие выводы:

1) наиболее распространенными экономическими преступлениями являются фишинг, «социальная инженерия», хакинг, что обусловлено развитием современного общества и используемых цифровых технологий;

2) по величине ущерба следует выделить следующие экономические преступления: «социальную инженерию», оффшорные схемы, программы-вымогатели, поскольку их использование предполагает мгновенное аккумулирование значительных денежных средств;

3) наименее рискованными являются такие экономические преступления, как программы-вымогатели, межсайтовый скриптинг и «социальная инженения», что обусловлено очень низкой вероятностью вычислить субъект экономического преступления;

4) по скорости получения выгоды лидерами являются финансовые пирамиды, «кража личности», «социальная инженерия», офшорные схемы, программы-вымогатели;

5) по количеству участников наиболее многочисленные это – финансовые пирамиды, офшорные схемы, «социальная инженерия».

Ключевую роль в расследовании киберпреступлений, финансового мошенничества и корпоративного шпионажа играет такая область знаний, как цифровая криминалистика. Цифровая криминалистика – это направление кибербезопасности, охватывающее совокупность методов и технологий, направленных на выявление, анализ и документирование цифровых следов преступлений (Яковлев 2018).

Предпосылка № 4. Технологический прогресс, стремительное развитие которого также стремительно меняет характер преступлений в бизнес-среде.

Ключевую роль в расследовании киберпреступлений, финансового мошенничества и корпоративного шпионажа играет такая область знаний, как цифровая криминалистика.

Цифровая криминалистика – это направление кибербезопасности, охватывающее совокупность методов и технологий, направленных на выявление, анализ и документирование цифровых следов преступлений (Яковлев 2018).

Таблица 3

Результаты ранжирования форм экономических преступлений применительно к онлайн-бизнесу по ряду критериев

Table 3

Results of ranking the forms of economic offences in relation to online business by a number of criteria

Формат преступления	Критерии по				
	распространенности	величине ущерба	уровню риска быть пойманным	скорости получения выгоды	количеству участников
Фишинг	1	4	9	4	5
Хакинг	3	6	8	6	7
Криптоджекинг	8	9	6	8	6
Спуфинг	5	10	7	7	8
Финансовые пирамиды	4	8	4	1	1
Оффшорные схемы	10	2	5	2	2
Программы-вымогатели	6	3	12	3	10
Межсайтовый скриптинг	12	11	11	4	11
«Кража личности»	11	5	7	2	4
«Социальная инженерия»	2	1	10	2	3
DDoS-атаки	7	7	6	5	12
Black Hat SEO	9	12	6	6	9

Источник: составлено авторами.

ЗАКЛЮЧЕНИЕ

На основании проведенного исследования сформулируем основные задачи цифровой криминалистики.

1. Выявление цифровых следов преступной деятельности – анализ интернет-трафика, логов серверов, файловых систем и облачных хранилищ.

2. Раскрытие сложных финансовых схем – использование аналитики больших данных (*Big Data*) и машинного обучения для идентификации аномальных транзакций.

3. Восстановление удаленной информации – извлечение данных с зашифрованных носителей, восстановление стертых файлов.

4. Анализ криптовалютных транзакций – отслеживание движения цифровых активов, выявление схем отмывания денег через блокчейн.

5. Доказательная база для судебных разбирательств – формирование отчетов и экспертных заключений, пригодных для использования в суде.

Цифровая криминалистика активно применяется правоохранительными органами, финансовыми регуляторами и частными компаниями для расследования преступлений в бизнес-среде.

Современные технологии и анализ больших данных (*Big Data*) помогают в борьбе с преступностью в бизнесе. Они являются полезным инструментом для работы с элементами, ориентированными на большие данные, представляющими интерес для правоохранительных органов. Модели нейронных сетей для прогнозирования конкретных видов преступлений с использованием информации о местоположении и времени разработаны для демонстрации применения их в своей деятельности органами внутренних дел (Архипов и др. 2024).

Основные направления применения искусственного интеллекта и *Big Data* в расследованиях:

а) финансовый мониторинг – автоматический анализ миллиона транзакций в режиме реального времени для выявления подозрительных операций;

б) блокчейн-аналитика – отслеживание движения криптовалютных активов и выявление подозрительных закономерностей и преступных схем;

в) алгоритмы поведенческого анализа – обнаружение необычных действий сотрудников, связанных с корпоративным мошенничеством;

г) распознавание фальсификаций – анализ цифровых документов, выявление подделок и фальшивых отчетов.

Применение таких технологий снижает нагрузку на экспертов и повышает эффективность расследований. Однако преступники также используют искусственный интеллект для создания более сложных схем мошенничества, что требует постоянного совершенствования аналитических инструментов.

Поскольку преступления в бизнес-среде носят транснациональный характер, борьба с цифровыми преступлениями требует международного сотрудничества. В настоящее время действуют несколько глобальных инициатив (Kiliç 2020): *FATF* (*Financial Action Task Force*) – разработка стандартов по борьбе с отмыванием денег и финансированием терроризма; *CRS* (*Common Reporting Standard*) – международный обмен налоговой информацией между государствами; Европол и Интерпол – совместные расследования транснациональных экономических преступлений; регуляторные инициативы ЕС и США – законы о борьбе с мошенничеством в сфере цифровых активов (*MiCA*, *AMLD*, *FinCEN*).

Эти меры помогают минимизировать риски цифровых преступлений, однако постоянное развитие технологий требует дальнейшего совершенствования механизмов контроля.

Таким образом, цифровизация бизнеса создает как новые возможности для экономического развития, так и серьезные вызовы в сфере экономической безопасности. Развитие цифровых платформ и трансграничное расширение бизнеса, использование криптовалют и децентрализованных финансов усложняет работу правоохранительных органов. Однако развитие цифровой криминалистики, аналитики *Big Data* и международного сотрудничества позволит эффективно противодействовать преступлениям в бизнес-среде.

СПИСОК ИСТОЧНИКОВ / REFERENCES

Авагян А. А., Мирзоян М. А., Кабанова Н. А. Проблема финансовых пирамид и современных способов мошенничества на финансовых и криптовалютных рынках // *Вестник евразийской науки* : сетевое издание. 2024. Т. 16, № s4. URL: https://esj.today/PDF/05FAVN424.pdf.

Avagyan, Anna A., Milena A. Mirzoyan, and Natalia A. Kabanova. 2024. “The problem of financial pyramids and modern methods of fraud in financial and cryptocurrency markets” [The problem of financial pyramids and modern methods of fraud in the financial and cryptocurrency markets] (In Russ.). *Vestnik yevraziyskoy nauki [Bulletin of Eurasian Science]* 16, no. s4. https://esj.today/PDF/05FAVN424.pdf.

Арженовский С. В., Бахтеев А. В., Синявская Т. Г. Комплекс мер по противодействию угрозам национальной безопасности России в сфере аудита // *Финансовые исследования*. 2021. № 3 (72). С. 22–29.

Arzhenovsky, Sergey V., Andrey V. Bakhteev, and Tatiana G. Sinyavskaya. 2021. “A Kompleks mer po protivodeystviyu ugrozam natsional'noy bezopasnosti Rossii v sfere audita” [“Complex of Measures to Counter Threats of the Russian National Security in Audit”] (In Russ.). *Finansovyye issledovaniya [Financial research]* 72, no. 3 (March–April): 22–9.

Архипов Д. Д., Гарцева Ю. Ю., Миллер В. Ю. К вопросу применения цифровой криминалистики в современных условиях // *Азиатско-тихоокеанский регион: экономика, политика, право*. 2024. Т. 26, № 3. С. 158–168. https://doi.org/10.24866/1813-3274/2024-3/158-168.

Arkhipov, Danila D., Yulia Yu. Gartseva, and Viktor Yu. Miller. 2024. “K voprosu primeneniya tsifrovoy kriminalistiki v sovremennykh usloviyakh [“On the issue of applying digital forensics in modern conditions.”] *Aziatsko-tikhookeanskiy region: ekonomika, politika, pravo [Asia-Pacific region: economics, politics, law]* 26, no. 3: 158–68. https://doi.org/10.24866/1813-3274/2024-3/158-168.

Вакутин А. А. «Беловоротничковая» преступность Э. Сатерленда: теория, не потерявшая актуальности // *Вестник Сибирского юридического института МВД России*. 2020. № 2 (39). С. 80–84. https://doi.org/10.51980/2542-1735_2020_2_80.

Vakutin, Artem A. 2020. ""Belovorotnichkovaya" prestupnost' E. Saterlenda: teoriya, ne poteryavshaya aktual'nosti" ["White-collar" crime of E. Sutherland: a theory that has not lost its relevance"] (In Russ.). *Vestnik Sibirskogo yuridicheskogo instituta MVD Rossii [Bulletin of the Siberian Law Institute of the Ministry of Internal Affairs of Russia]* 39, no. 2: 80–84. https://doi.org/10.51980/2542-1735_2020_2_80.

Варакса Н. Г., Бехбудова Ф. Ф. Финансовые пирамиды как угроза финансовой безопасности граждан // *Давыдовские чтения. Тренды и перспективы цифровой экономики: финансовые технологии и безопасность* : материалы II Всероссийской научно-практической конференции, г. Орел, 20–21 июня 2023 г. Орел : Орловский государственный университет им. И. С. Тургенева, 2023. С. 177–185.

Varaksa, Natalia G., and Flora F. Bekhbudova. 2023. "Finansovyye piramidy kak ugroza finansovoy bezopasnosti grazhdan" ["Financial pyramids as a threat to the financial security of citizens"] (In Russ.). In: *Davydovskiye chteniya. Trendy i perspektivy tsifrovoy ekonomiki: finansovyye tekhnologii i bezopasnost' [David's readings. Trends and prospects of the digital economy: financial technologies and security]*, 177–85. Orel: Oryol State University named after I. S. Turgenev.

Власова С. В. Теоретико-методологическая модель правовой организации противодействия экономической преступности в условиях цифровизации // *Вопросы российского и международного права*. 2023. Т. 13, № 1А-2А. С. 334–341. https://doi.org/10.34670/AR.2023.66.92.043.

Vlasova, Svetlana V. 2023. "Teoretiko-metodologicheskaya model' protivodeistviya ekonomicheskoi prestupnosti v usloviyakh tsifrovizatsii" ["Theoretical and methodological model of the legal organization of countering economic crime in the context of digitalization"] (In Russ.). *Voprosy rossiiskogo i mezhdunarodnogo prava [Matters of Russian and International Law]* 13, no. 1A-2A: 334–41. https://doi.org/10.34670/AR.2023.66.92.043.

Воловик А. М. Экономика искусственного интеллекта: тенденции, комплаенс, глобальное влияние // *Экономическая безопасность*. 2024. Т. 7, № 9. С. 2239–2254. https://doi.org/10.18334/ecsoc.7.9.121752.

Volovik, Alexander M. 2024. "Ekonomika iskusstvennogo intellekta: tendentsii, komplayens, global'noye vliyaniye" [Economics of artificial intelligence: trends, compliance, global influence] (In Russ.). *Ekonomicheskaya bezopasnost' [Economic security]* 7, no. 9: 2239–54. https://doi.org/10.18334/ecsoc.7.9.121752.

Воротникова А. С. Отдельные закономерности совершения современных экономических преступлений в киберпространстве // *Гуманитарные, социально-экономические и общественные науки*. 2024. № 12. С. 150–154. https://doi.org/10.24412/2220-2404-2024-12-5.

Vorotnikova, Anna S. 2024. "Otdel'nyye zakonomernosti sovershenіya sovremennykh ekonomicheskikh prestupleniy v kiberprostranstve" [Certain patterns of committing modern economic crimes in cyberspace] (In Russ.). *Gumanitarnyye, sotsial'no-ekonomicheskiye i obshchestvennyye nauki [Humanities, socio-economic and social sciences]*, no. 12: 150–54. https://doi.org/10.24412/2220-2404-2024-12-5.

Есаков Г. А., Саушкин Д. В. Умысел в налоговых преступлениях и конструкция продолжаемого преступления // *Уголовное право*. 2020. № 4. С. 15–20.

Esakov, Gennady A., and D. V. Saushkin. 2020. "Umysel v nalogovykh prestupleniyakh i konstruktsiya prodolzhayemogo prestupleniya" [Intent in tax crimes and the structure of a continuing crime] (In Russ.). *Ugolovnoye pravo [Criminal Law]*, no. 4: 15–20.

Фалина Н. В., Каплиев А. Ю., Шамрай К. Е. Совершенствование системы мониторинга криминализации экономики в условиях обеспечения экономической безопасности // *Естественно-гуманитарные исследования*. 2023. № 5 (49). С. 265–271.

Falina, Natalia V., A. Yu. Kapliyev, and Kirill E. Shamrai. 2023. "Sovershenstvovaniye sistemy monitoringa kriminalizatsii ekonomiki v usloviyakh obespecheniya ekonomicheskoy bezopasnosti" ["Improving the system of monitoring the criminalization of the economy in the context of ensuring economic security"] (In Russ.). *Yestestvenno-gumanitarnyye issledovaniya [Natural Sciences and Humanities Research]* 49, no. 5: 265–71.

Федотов А. А. Экономические и иные мотивы в теориях причин преступности // *Международный журнал гуманитарных и естественных наук*. 2023. № 9-2 (84). С. 243–249. https://doi.org/10.24412/2500-1000-2023-9-2-243-249.

Fedotov, Artem A. 2023. "Ekonomicheskiye i inyye motivy v teoriyakh prichin prestupnosti" ["Economic and other motives in theories of the causes of crime"] (In Russ.). *Mezhdunarodnyy zhurnal gumanitarnykh i yestestvennykh nauk [International Journal of Humanities and Natural Sciences]* 84, no. 9-2: 243–49. https://doi.org/10.24412/2500-1000-2023-9-2-243-249.

Филатова Т. А., Дымшакова А. А., Лашманова Е. Е. Роль экономической экспертизы в системе экономической безопасности страны // *Актуальные вопросы научных исследований* : сборник статей V Международной научно-практической конференции, г. Саратов, 10 декабря 2023 г. / отв. ред. И. О. Болдырева. Саратов : Амирит, 2024. С. 331–342.

Filatova, Tatiana A., A. A. Dymshakova, and E. E. Lashmanova. 2024. "Rol' ekonomicheskoy ekspertizy v sisteme ekonomicheskoy bezopasnosti strany" ["The Role of Economic Expertise in the System of Economic Security of the Country"] (In Russ.). In: *Aktual'nyye voprosy nauchnykh issledovaniy [Current issues of scientific research]*, edited by I. O. Boldyreva 331–42. Saratov: Amirit.

Яковлев А. Н. Цифровая криминалистика как фактор защиты цифровой экономики // *Криминалистика в условиях развития информационного общества (59-е ежегодные криминалистические чтения)* [электронный ресурс] : сборник статей Международной научно-практической конференции, г. Москва, 18 мая 2018 г. Москва : Академия управления МВД России, 2018. С. 325–331.

Yakovlev, Alexey N. 2018. “Tsifrovaya kriminalistika kak faktor zashchity tsifrovoy ekonomiki” [Digital forensics as a factor in protecting the digital economy”] (In Russ.). In: *Kriminalistika v usloviyakh razvitiya informatsionnogo obshchestva (59-ye yezhegodnyye kriminalisticheskiye chteniya) [Forensic science in the context of the development of the information society (59th annual forensic readings)]* 325–31. Moscow: Academy of Management of the MIA of the Russian Federation.

Becker G. S. Crime and Punishment: An Economic Approach // *Journal of Political Economy*. 1968. № 76 (2). P. 169–217.

Becker, Gary S. 1968. “Crime and Punishment: An Economic Approach.” *Journal of Political Economy* 76, no. 2 (March-April): 169–217.

Kiliç B. I. The Effects of Big Data on Forensic Accounting Practices and Education // *Contemporary Issues in Audit Management and Forensic Accounting*. 2020. Vol. 102. P. 11–26. https://dx.doi.org/10.1108/s1569-375920200000102005.

Kiliç, Burcu I. 2020. “Effects of Big Data on Forensic Accounting Practices and Education.” *Contemporary issues in audit management and forensic accounting*, 102: 11–26. https://dx.doi.org/10.1108/s1569-375920200000102005.

Sutherland E. H. *Principles of Criminology* (4th ed.). Philadelphia : J. B. Lippincott Company, 1947. 645 p.

Sutherland, Edwin H. 1947. *Principles of Criminology* (4th ed.) 645. Philadelphia : J. B. Lippincott Company.

Авторами внесен равный вклад в написание статьи.
Авторы заявляют об отсутствии конфликта интересов.

The authors have made an equal contribution to the writing of the article.
The authors declare no conflicts of interests.