

Анастасия Олеговна Лёвкина

кандидат экономических наук, доцент, профессор кафедры экономической безопасности, системного анализа и контроля Тюменского государственного университета, г. Тюмень, a.o.lyovkina@utmn.ru

Екатерина Андреевна Брюханова

студентка специальности «Экономическая безопасность» Тюменского государственного университета, г. Тюмень, katya.bryuxanova.04@inbox.ru

Диана Николаевна Митина

студентка специальности «Экономическая безопасность» Тюменского государственного университета, г. Тюмень, m.diana.00@bk.ru

ФИНАНСОВЫЕ ПРЕСТУПЛЕНИЯ В ОРГАНИЗАЦИЯХ: КЛАССИФИКАЦИЯ И СПОСОБЫ ИХ НЕЙТРАЛИЗАЦИИ

Аннотация. В статье рассматривается проблема финансовых преступлений в организациях, обосновывается ее актуальность в контексте экономической безопасности. Анализируется законодательство РФ в области противодействия мошенничеству в предпринимательской деятельности, в частности, статьи 159.3 УК РФ и 159.6 УК РФ. Представлены статистические данные о финансовых преступлениях и осужденных. Особое внимание уделяется типичным схемам обмана в корпоративных финансах, а также предлагаются эффективные стратегии по обнаружению и защите от подобных махинаций в деловой среде.

Ключевые слова: финансовые преступления, корпоративное мошенничество, уголовный кодекс, правонарушение, обман и хищение, предпринимательская деятельности и бизнес.

Anastasia Olegovna Levkina

Candidate of Sciences (Economics), Professor of the Department of Economic Security, System Analysis and Control of Tyumen State University, Tyumen, a.o.lyovkina@utmn.ru

Ekaterina Andreevna Bryukhanova

Student of the specialty "Economic Security" of Tyumen State University, Tyumen, katya.bryuxanova.04@inbox.ru

Diana Nikolaevna Mitina

Student of the specialty "Economic Security" of Tyumen State University, Tyumen, m.diana.00@bk.ru

FINANCIAL CRIMES IN ORGANIZATIONS: CLASSIFICATION AND WAYS TO NEUTRALIZE THEM

Abstract. The article examines the problem of corporate financial fraud in Russia and substantiates its relevance in the context of economic security. The article analyzes the legislation of the Russian Federation in the field of combating fraud in business, in particular, Articles 159.3 of the Criminal Code and 159.6 of the Criminal Code. Statistical data on crimes and convicts are presented. Special attention is paid to typical fraud schemes in corporate finance, and effective strategies for detecting and protecting against such frauds in the business environment are proposed.

Keywords: financial crimes, corporate fraud, criminal code, offense, deception and embezzlement, entrepreneurial activity and business.

Актуальность систематизации и классификации финансовых преступлений обусловлена необходимостью эффективно противостоять угрозам экономической безопасности государства, связанным с повышением уровня криминализации экономики. Согласно государственной статистике, количество преступлений экономической направленности увеличилось. Так, в 2024 году за

январь-март было зарегистрировано 36 701 преступление, а за тот же период 2025 года — 40 061 [1]. Такая ситуация требует от государства формирования более сильной культуры законности в бизнесе и других видах хозяйственной деятельности наряду с повышением эффективности применяемых инструментов реагирования и профилактики в сфере экономических преступлений, особенно в сфере уголовного права.

Получение прибыли выступает ключевой задачей предпринимательства, структуры которого представляют собой систему разнообразных действий, включающих поставку продукции, выполнение работ и другие виды активности. Хищение имущества, совершенное обманным путем в сфере предпринимательства, карается статьей 159 УК РФ [2].

Основными условиями для применения статьи 159 УК РФ являются:

- умышленное неисполнение обязанностей, предусмотренных заключенным договором;
- прошедшее процедуру официальной регистрации лицо, являющееся предпринимателем (в любой форме), которому уже исполнилось 16 лет;
- трудовые отношения между потерпевшим и преступником были официально зарегистрированы посредством соответствующего договора;
- во время заключения договора злоумышленник в принципе не собирался как-либо выполнять свои законные обязанности.

Весной 2018 г. были внесены следующие законодательные изменения: в ст. 158 УК РФ введен квалифицирующий признак — кража с банковского счета, а равно в отношении электронных денежных средств (далее — ЭДС) при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ, снижены пороговые значения крупного размера с 1,5 млн руб. до 250 тыс. руб., особо крупного — с 6 млн руб. до 1 млн руб. в ст. 159.3 (мошенничество с использованием электронных средств платежа), 159.6 (мошенничество в сфере компьютерной информации); ч. 3 ст. 159.6 дополнена новым квалифицирующим признаком — мошенничество в сфере компьютерной информации, совершенное с банковского счета, а равно в отношении ЭДС.

В последнее время Россия столкнулась с беспрецедентным количеством и разнообразием форм электронного мошенничества. Статья 159.3 Уголовного кодекса Российской Федерации предусматривает ответственность за мошенничество с использованием электронных средств платежа. Ниже представлены данные о количестве зарегистрированных преступлений и осужденных лиц по данной статье за последние годы (рис. 1).

Статья 159.6 Уголовного кодекса Российской Федерации предусматривает ответственность за мошенничество в сфере компьютерной информации. Согласно имеющимся данным, количество осужденных по данной статье за последние годы значительно снизилось: 2022 год: 54 человека, 2023 год: 34 человека, 2024 год: 29 человек (рис. 2).

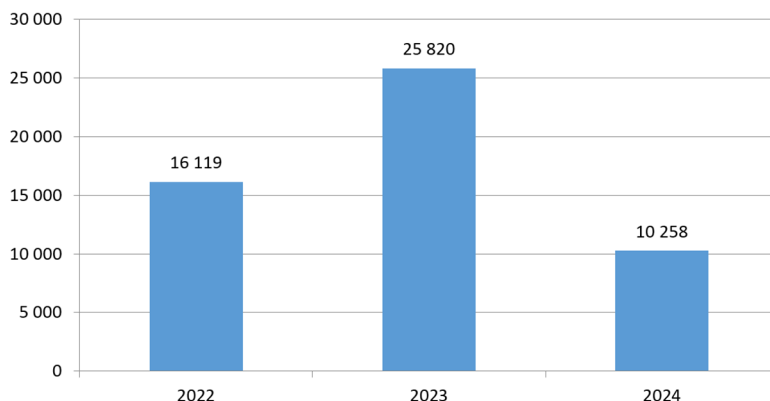


Рис. 1. Количество зарегистрированных преступлений по ст. 159.3 УК РФ за 2022–2024 гг.

Источник: [3].

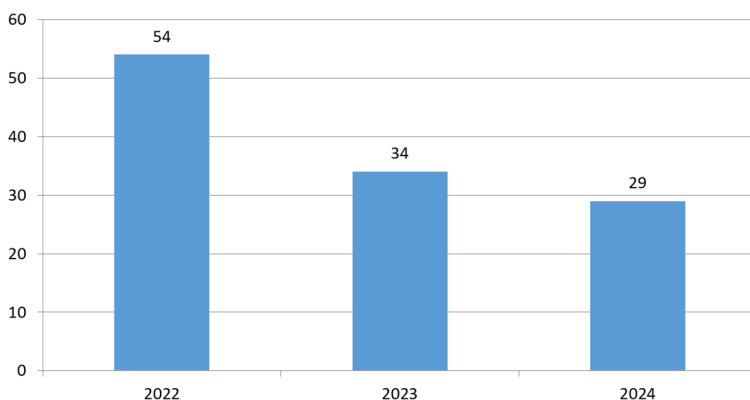


Рис. 2. Количество осужденных по ст. 159.6 УК РФ за 2022–2024 гг.

Источник: [3].

Показатели по количеству осужденных по ст. 159.6 УК РФ свидетельствуют о снижении числа осужденных по данной статье практически в 2 раза за период 2022–2024 гг. Однако следует учитывать, что данные могут быть неполными из-за высокого уровня латентности подобных преступлений, многоплановых сложностей их выявления, расследования и привлечения к ответственности.

Исследование показало, что за прошедшие 24 месяца около 50% организаций в России стали жертвами криминальных действий экономического характера. Взяточничество и коррупционные схемы, махинации при закупке товаров и услуг, а также неправомерное завладение активами компаний оказались наиболее типичными формами экономических преступлений, с которыми столкнулся российский бизнес [4, с. 558].

Надежный способ профилировать финансовые преступления в организации и выявить признаки совершенных уголовных преступлений является

независимая экспертиза финансово-хозяйственной деятельности компании. Документация бухгалтерского учета и контрактные соглашения с партнерами и кредиторами служат основным источником для выявления противоправных действий. Отсутствие обоснования в принятии финансовых решений представляет собой главное доказательство неправомерного поведения. Пострадавшие от противозаконных действий нарушителей имеют полное право обратиться за защитой в правоохранительные органы. Но для этого необходимо написать соответствующее заявление (скачать заявление) и предпринимать следующие действия:

1. Направить заранее подготовленное заявление в полицейский участок, обслуживающий территорию, где проживаете вы или где ведет свою деятельность финансовый преступник.

2. В случае необходимости проверить предпринимателя (или сотрудника) на предмет мошенничества, следует направить запрос в прокуратуру. Именно там могут провести расследование и установить факт противоправных действий.

3. После завершения досудебного урегулирования конфликта, направленного на возможное решение спора в претензионном порядке, а также собрав необходимые доказательства правонарушения и установив виновное лицо, подлежащее привлечению к ответственности, возможно инициировать судебное производство с готовым иском заявлением.

Законодательство предусматривает различные квалифицирующие признаки для классификации мошенничества, включая размер причиненного ущерба и коллективное совершение преступления по предварительному соглашению. Однако части 5-7 статьи 159 Уголовного кодекса РФ ограничиваются лишь указанием на масштаб нанесенного ущерба. Такой ограниченный подход вызывает сомнения в своей обоснованности, поскольку в сфере предпринимательства преступный умысел может формироваться у нескольких участников одновременно.

Так, например, Кировский районный суд Томска вынес обвинительный приговор по делу председателя правления ТСЖ «Х». Гражданин Х. был признан виновным по ч.1 ст.165 УК РФ за причинение крупного имущественного ущерба собственникам квартир. Злоупотребляя полномочиями и используя доверенности членов товарищества, он намеренно искажал информацию о тарифах. Собственникам была предоставлена недостоверная информация относительно расчета и размера платежей за содержание, ремонт и отопление общедомового имущества. Манипулируя доверием жильцов, председатель нанес существенный материальный ущерб членам ТСЖ «Х» [5, с. 17].

В современном контексте, когда общественная опасность мошеннических действий значительно возросла, этот вид правонарушения занял особую нишу в спектре имущественных преступлений. Для эффективного противодействия подобным правонарушениям важно совершенствовать методы их выявления и пресечения. Ключевым аспектом в борьбе с мошенничеством в предпринимательской сфере является точная идентификация его отличительных характеристик. Правильное определение способов совершения, мотивационных факторов и целевых установок позволяет провести четкую демаркационную линию

между мошенничеством и другими противоправными деяниями. Формирование ясных правовых позиций также необходимо для корректной квалификации и отграничения от смежных составов преступлений [6, с. 231].

На основании анализа кейсов анализа индуктивным методом нами были выделены первоочередные обязательные меры для предотвращения основных типов мошенничества в бизнес-среде. Основные типы мошенничества были выделены на основании анализа современной научно-учебной и публицистической литературы:

1. Слив конфиденциальной информации.

Согласно статистике, подавляющее большинство случаев компрометации данных (около 95%) реализуется самым примитивным способом. Сотрудники в рабочие часы, используя корпоративные компьютеры, сохраняют необходимые файлы на десктоп, после чего пересылают их на свои персональные электронные адреса. Такой простой и явный метод утечки конфиденциальной информации остается наиболее распространенным, как свидетельствуют официальные источники. Что произойдет с информацией после того, как она окажется в руках недобросовестного работника — неизвестно. Он может, например, использовать ее при трудоустройстве к конкурентам или выставить на продажу в даркнете. Хотя злоумышленники не так часто прибегают к загрузке данных в облачные хранилища, распечатке документов, передаче через мессенджеры и социальные сети или копированию на USB-накопители.

Для эффективной защиты информации первым шагом является идентификация уязвимых данных. Необходимо создать исчерпывающий список сведений, требующих особой охраны. Важно определить, какие именно элементы представляют наибольший риск при утечке. Коммерческая и иная конфиденциальная информация может включать различные компоненты: от технологических процессов производства до финансовой отчетности и клиентских баз. Анализ степени уязвимости каждого типа данных позволит разработать соответствующие защитные меры [7, с. 46]. Современные ПО, такие как «Стахановец», «Kickidler», «Инсайдер» способны проанализировать все уязвимые места в автоматическом режиме и затем выдать отчет, где будет обозначена «ахиллессова пята» организации.

Контроль буфера обмена обычно является достаточной мерой для предотвращения несанкционированной передачи данных. Служба безопасности организации, как правило, получает автоматические уведомления в случаях, когда работник осуществляет копирование файлов на съемные носители или прикрепляет документы к электронным сообщениям.

2. Откаты.

Исследование HeadHunter [8] выявило, что значительная часть сотрудников различных сфер склонна к коррупционным действиям. Особенно заметна эта тенденция среди представителей автобизнеса, юридической отрасли и административных работников. Однако наибольшую готовность принять неправомерное вознаграждение демонстрируют специалисты по продажам — каждый третий из них не готов отказаться от предложенного отката.

Мониторинг коммуникаций персонала представляет серьезную проблему, особенно для крупных организаций. Полный контроль всей корреспонденции

требует значительного расширения отдела безопасности, что экономически нецелесообразно. Вместо этого многие корпорации успешно внедряют систему фильтрации сообщений на основе определенных терминов и фраз. Такой подход позволяет эффективно выявлять потенциально проблемный контент без необходимости тотального наблюдения.

Данная методика позволяет осуществлять автоматическое наблюдение за всеми письмами. Система выявляет работников, которые негативно отзываются о компании или планируют уйти. Сообщения, содержащие такие термины как "вознаграждение", "взятка", "откат" и подобные, автоматически классифицируются как подозрительные.

Недавний случай в Германии показал, как компания смогла уволить программиста после установки специального трекера на его клавиатуру. Это лишь один пример использования программ-агентов, способных перехватывать коммуникации сотрудников. Такие инструменты обходят даже шифрование мессенджеров, фиксируя непосредственно нажатия клавиш при наборе сообщений [9, с. 81].

3. Фальсификация документов.

Манипуляции с аналитическими данными и фальсификация отчетов становятся соблазном для сотрудников, когда их материальное поощрение напрямую связано с показателями результативности. Однако любое искажение цифровой информации оставляет характерные следы. Компьютерные алгоритмы способны обнаружить эти незаметные для человека аномалии в статистике, даже если визуально они неразличимы. Стремление получить премии и бонусы толкает работников на подтасовку данных, но современные технологии делают такие махинации все более рискованными.

В эпоху мобильных технологий руководители получают возможность отслеживать перемещения персонала через специальные приложения. Особенно это решение ценно для организаций с курьерской доставкой и выездными офисами продаж, обеспечивая постоянный контроль над сотрудниками. Что касается фальсификации отчетных данных, современные компьютерные алгоритмы способны обнаружить даже незаметные человеческому глазу следы постороннего вмешательства. Любые попытки подделки неизбежно оставляют цифровой отпечаток, который легко выявляется специализированными программами [10, с. 89].

4. Сторонний бизнес на рабочем месте.

Руководство часто упускает из виду, что снижение продаж может сигнализировать о серьезной проблеме. Особенно уязвимы удаленные представительства и региональные филиалы, где контроль ослаблен. Некоторые работники организуют собственные коммерческие предприятия, фактически используя ресурсы работодателя. Они не только эксплуатируют корпоративные базы клиентов, но и активно склоняют заказчиков к сотрудничеству напрямую, ведя параллельную деловую активность прямо на рабочем месте.

Так, работница фирмы, специализирующейся на подготовке тендерной документации, решив подзаработать, начала тайно предлагать бывшим клиентам компании идентичные услуги напрямую, но дешевле. Вся прибыль от этой неофициальной деятельности поступала исключительно в ее карман. Примеча-

тельно, что для выполнения своих личных заказов женщина использовала корпоративные ресурсы: рабочее время, офисное место, специализированные программы, электронную почту компании, цифровую подпись и служебный мобильный телефон [11].

В таких ситуациях для выявления причин снижения продаж, не связанных с эмоциональным выгоранием сотрудника, рекомендуется использовать анализ поведенческих паттернов и методику контроля отклонений с оценкой рисков. Заметные изменения в поведении персонала часто указывают на то, что работники могут развивать собственные бизнес-проекты параллельно с основной деятельностью.

Сотрудники, вызывающие подозрения у руководства, могут быть под наблюдением с помощью специальных программ мониторинга. Эти инструменты фиксируют увеличение активности в электронной переписке, а также отслеживают продолжительность веб-серфинга и посещение конкретных сайтов. Руководители имеют возможность детально изучить действия подчиненных как в реальном времени, так и ретроспективно [5, с. 17]. DLP-системы (Data Leak Prevention) представляют собой современные инструменты для защиты конфиденциальной информации и предотвращения ее утечек, обеспечивая мониторинг, контроль и управление за важными данными организации. Одним из лидеров российского рынка DLP-систем является InfoWatch — сервис, работающий в 26 странах, который предлагает решения для защиты информации и управления рисками утечек. Также на их сайте регулярно публикуются международные новости утечек информации, статистика и аналитические отчеты по различным инцидентам.

Таким образом, необходимо отметить, что мошенничество в РФ является серьезной проблемой, над которой нужно системно работать на всех уровнях управления. Хотя корень проблемы формирования добросовестного бизнес-общества лежит преимущественно в человеческом факторе, необходимы существенные усилия одновременно в разных сферах. В социальной и образовательной сферах необходимы меры по воспитанию личной порядочности, ответственности за соблюдение национальных интересов и законодательства и следованию общечеловеческим этическим принципам. В правовой и законодательной сфере — меры по усилению контроля за деятельностью государственной власти и местного самоуправления, расширение перечня составов преступлений, обязательное информирование клиентов финансовыми организациями о рисках и способах защиты от мошенничества.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Количество преступлений экономической направленности, зарегистрированных в отчетном периоде // Единая межведомственная информационно-статистическая система: сайт. — URL: <https://fedstat.ru/indicator/3622> (дата обращения: 21.04.2024).
2. Уголовный кодекс Российской Федерации: от 13.06.1996, № 63-ФЗ: ред. от 21.04.2025 // Собрание законодательства РФ. 1996 г. № 25. Ст. 159 // Консультант-Плюс: надежная правовая поддержка: сайт. — URL: https://www.consultant.ru/document/cons_doc_LAW_10699/8012ecdff64b7c9cfd62e90d7f55f9b5b7b72b755/ (дата обращения: 21.04.2024).
3. Статистические данные // Генеральная прокуратура РФ: сайт. — URL: <https://epp.genproc.gov.ru/web/gprf/activity/statistics> (дата обращения: 21.04.2024).

4. Сащенко А.Ю. Способы предупреждения экономических преступлений на производственных предприятиях / А.Ю. Сащенко, Е.И. Пикула // Интеллектуальная инженерная экономика и индустрия 5.0 (Инпром): сборник трудов VIII Международной научно-практической конференции. — Санкт-Петербург «Издательство», 2023. — С. 558-560.
5. Абдулаева А.А. Мошенничество в бизнесе: состояние и меры по снижению / А.А. Абдулаева // Модернизация экономических систем: политика, экономика, общество и право: материалы IV Международной научно-практической конференции. — Махачкала: «Издательство», 2020. — С. 17-23.
6. Попова А.А. Финансовое мошенничество как угроза экономической безопасности предпринимательской деятельности: особенности и классификационные признаки / А.А. Попова, М.К. Скороварова, В.О. Бессарабов // Финансовый контроль и казначейское сопровождение целевых средств: перспективы развития в условиях цифровизации: материалы I Международной научно-практической интернет-конференции. — Донецк: «Издательство», 2023. — С. 231-235.
7. Алыев Р.Т. О причинной составляющей уголовной ответственности за преступления в сфере предпринимательства / Р.Т. Алыев // Юридический журнал. — 2024. — № 1. — С. 46-50.
8. HeadHunter выяснил, в каких сферах труда в России процветает коррупция // КЛОПС: сайт. — URL: <https://klops.ru/news/obschestvo/131404-headhunter-vyyasnil-v-kakih-sferah-truda-v-rossii-protsvetaet-korrupsiya> (дата обращения: 21.04.2024).
9. Чупрова А.Ю. Проблемы правовой оценки легализации преступных доходов: компаративистский аспект / А.Ю. Чупрова, Е.В. Фоменко, З.В. Каменева // Правовая культура. — 2023. — № 1 (52). — С. 73-81.
10. Капустина Н.В. Корпоративное мошенничество как угроза экономической безопасности организации / Н.В. Капустина // Вестник евразийской науки. — 2024. — Т. 16. — № S1. — С. 89.
11. Определение ВС от 28.01.2019 № 18-КГ18-225 // Время бухгалтера: сайт. — URL: <https://www.v2b.ru/documents/opredelenie-vs-rf-ot-28-01-2019-18-kg18-225/> (дата обращения: 21.04.2024).