

Вестник Евразийской науки / The Eurasian Scientific Journal <https://esj.today>

2023, Том 15, № s1 / 2023, Vol. 15, Iss. s1 <https://esj.today/issue-s1-2023.html>

URL статьи: <https://esj.today/PDF/15FAVN123.pdf>

DOI: 10.15862/15FAVN123 (<https://doi.org/10.15862/15FAVN123>)

**Ссылка для цитирования этой статьи:**

Гладков, Д. О. Современные тенденции в области противодействия корпоративному мошенничеству / Д. О. Гладков, Р. К. Бадма-Халгаев, Е. С. Сеницын // Вестник евразийской науки. — 2023. — Т. 15. — № s1. — URL: <https://esj.today/PDF/15FAVN123.pdf> DOI: 10.15862/15FAVN123

**For citation:**

Gladkov D.O., Badma-Khalgaev R.K., Sinityn E.S. Current trends in countering corporate fraud. *The Eurasian Scientific Journal*. 2023; 15(s1): 15FAVN123. Available at: <https://esj.today/PDF/15FAVN123.pdf>. (In Russ., abstract in Eng.) DOI: 10.15862/15FAVN123

УДК 314

**Гладков Денис Олегович**

ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия  
E-mail: D9211121@yandex.ru

**Бадма-Халгаев Руслан Константинович**

ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия  
E-mail: tmntgogo@gmail.com

**Сеницын Егор Сергеевич**

ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия  
E-mail: egor.sinityn@mail.ru

## Современные тенденции в области противодействия корпоративному мошенничеству

**Аннотация.** В данной статье рассматривается вопрос, связанный с изучением современных тенденций в области противодействия корпоративному мошенничеству. Автором было дано описание ключевых аспектов, связанных с понятием корпоративного мошенничества, в том числе суть рассматриваемого понятия, его правовые характеристики, а также место данного явления в уголовной системе России. Важное место в данной работе отведено для анализа деятельности по противодействию корпоративному мошенничеству, причем данный процесс проводится как со стороны государства в лице отдельных институтов власти, так и со стороны самих организаций, проводящих внутренние проверки и другие мероприятия подобного рода. Автором был проведен анализ существующей законодательной базы, связанной с корпоративным мошенничеством и мошенничеством в экономической сфере, при этом сохранены принципы исторической преемственности и взаимосвязи между принимаемыми законами как внутри одного государства, так и в процессе перенимания отдельных пунктов другими странами. В данной работе также приведены примеры ситуаций, в которых не получается в полной мере применить методы, направленные на противодействие корпоративному мошенничеству, при этом в качестве основных причин автором выделены две группы, первая из которых относится к недостаточной проработке указанных методов, а вторая группа отражает трудности, которые возникают из-за самих организаций, на которые направлены эти методы. В заключительной части работы автором даны рекомендации по повышению эффективности применяемых мероприятий, направленных на противодействие корпоративному мошенничеству, а также по введению новых методов, способных снизить

негативные последствия от результатов отдельных проявлений корпоративного мошенничества, например присвоения активов.

**Ключевые слова:** корпоративное мошенничество; уголовная ответственность; внутренняя проверка; теневая экономика; противодействие мошенничеству; коррупция; Big Data

## Введение

Актуальность данной темы обоснована тем, что согласно докладу ACFE в результате корпоративного мошенничества «исчезает» более 3,7 триллионов долларов, что составляет 5 % от общего ВВП в 2021 году. Если применить аналогичный показатель к России, при условии, что ВВП составил 66,75 трлн рублей, то это свыше 3,3 трлн руб.

Целью данной работы является рассмотрение сложившихся тенденций в области противодействия корпоративному мошенничеству. При этом можно выделить следующие задачи:

1. Рассмотреть основные характеристики корпоративного мошенничества.
2. Описать принципы действия организаций по противодействию корпоративного мошенничества.
3. Изучить методы, применяемые для борьбы с корпоративным мошенничеством.
4. Дать рекомендации по дальнейшему противодействию корпоративному мошенничеству.

Объектом данного исследования выступает корпоративное мошенничество как социально-экономическое явление. Предметом — методы в области противодействия корпоративному мошенничеству.

## 1. Материалы и методы

Корпоративное мошенничество — «это хищение активов компании, осуществляемое обманным путем и характеризующееся умышленным воздействием на финансово-хозяйственную деятельность компании и системы по ее регистрации и анализу в целях совершения и (или) сокрытия мошеннических действий. Также к хищению активов тесно примыкает использование менеджментом и персоналом компании своего служебного положения с целью личного обогащения, осуществляемое за вознаграждение, но без фактического изъятия активов у компании (так называемая «неценовая коррупция»)». Это преступное деяние попадает по действие, как минимум, 4-х статей УК РФ: 158 «Кража», 159 «Мошенничество», 160 «Присвоение или растрата», 201 «Злоупотребление полномочиями». Однако стоит отметить, что компании чаще всего пытаются собственными силами решать подобные проблемы, не вынося ссор из «избы».

Существенный вклад в исследование вопросов корпоративного мошенничества внесли Скипин Д.Л. [1], Снимщикова И.В. [2], Телкова Е.А. [3]. При написании работы была использована отечественная и переводная учебная литература, в частности труды Агеева Л.С. [4], Долганов С.И. [5] и многих других научных деятелей, посвященные изучению тенденций в области противодействия корпоративному мошенничеству.

При написании работы использовались общенаучные методы познания, такие как системный подход, статистические методы обработки массивов информации, методы анализа и синтеза. Были широко использованы индуктивный и дедуктивный методы, а также сравнительный анализ.

## 2. Результаты и обсуждение

Американский социолог-криминолог Эдвин Х. Сазерленд впервые дал определение преступления связанных с мошенничеством непосредственно внутри корпораций — whit-collar crime. В это понятие он вложил тот факт, что это деяние совершается в сфере экономики представителями бизнеса, государства и других должностных лиц, которые имеют колоссальный ущерб в экономике страны, внутри которой зарегистрирована фирма [6].

Причину возникающей проблемы, можно понять, обратив внимание на то, откуда корпоративное мошенничество берет свои истоки. Любой бизнес является организмом, которому привычно развиваться в конкурентной среде. В свою очередь конкурентная среда работает по своим законам, в которой компании действуют в своих интересах, разделяясь между собой на две группы: «свой» и «чужие». Более того, внутри компании существует такая же тенденция: сотрудники делятся на те же две группы; активы компании создают свои противоречия: сотрудники, внутри компании, относящиеся к «чужим», имеющие доступ к капиталу компании, с большой вероятностью могут действовать в своих собственных интересах [7].

Было предпринято огромное количество попыток измерить уровень и частоту мошенничества, но так как провести достоверный опрос нелегко и, соответственно, составить валидные статистические данные невозможно, считается, что большинство актов мошенничества остается незамеченным. Кроме того, достаточно сложно отличить мошенничество от просто невнимательного ведения бухгалтерского учета. Тем не менее, существуют ключевые аспекты мошенничества, которые достоверно известны и легко выявляемы.

Мошенники, пользуясь оказанным доверием, могут присваивать части прибыли компании, среди которых могут быть как фиктивные счета, так и умышленное изменение платежных отчетов, а также сокрытие доходов; могут похищать активы компании, по итогу хищения которых компания и собственник капитала терпят убытки; могут способствовать коррупционной составляющей: к примеру, присваивать вознаграждения от третьих лиц в ущерб интересам компании; могут вносить заведомо ложные данные в бухгалтерскую и финансовую отчетность, скрывать следы мошеннических действий или изменять финансовую отчетность как в лучшую, так и в худшую сторону для обманного впечатления на инвесторов, кредиторов или для ухода от уплаты налогов [8].

На данной основе была создана компанией ACFE («Объединение сертифицированных специалистов по борьбе с хищениями») классификация корпоративного мошенничества компаний:

- Коррупция: конфликт интересов, взяточничество, предоставление необоснованных преимуществ, финансовое вымогательство.
- Присвоение активов: наличные денежные средства, товарно-материальные ценности и прочие активы.
- Мошенничество с финансовой отчетностью: завышение доходов/прибыли, занижение доходов/прибыли [9].

На современном этапе компании разрабатывают и внедряют различные методы противодействия корпоративному мошенничеству. Однако в компаниях часто возникает проблема с обработкой информационных потоков организации, например, из-за их большого объема, сложностью сбора и пр. В современном бизнесе наблюдается тенденция использования так называемых больших данных или Big Data для решения подобной проблемы. Часто проблема организации состоит не в том, что она создает огромные объемы данных, а в том, что доминирующая их составляющая представлена в формате, который не соответствует традиционному структурированному формату, к тому же, она хранится на разных источниках. Возникает ситуация, когда корпорация имеет доступ к огромному объему своих данных и не имеет необходимых инструментов, чтобы наладить между ними взаимосвязь. Учитывая то обстоятельство, что данные обновляются все чаще и чаще, получается, что традиционные методы анализа информации не способны обеспечить полный ее контроль. Этот факт и открывает путь технологиям Big Data.

Под термином Big Data подразумевается работа с информацией большого объема с разнообразной структурой, часто обновляемой и находящейся в различных источниках, в целях увеличений новых продуктов и повышения конкурентоспособности. Согласно определению консалтинговой компании Forrester Big Data — это «большие данные, объединяющие техники и технологии, которые извлекают смысл из данных на экстремальном пределе практичности». Также стоит отметить следующее определение: большие данные (Big Data) — серия подходов, инструментов и методов обработки, структурированных и неструктурированных данных как больших, так и малых объемов и значительного многообразия для получения воспринимаемых человеком результатов, эффективных в условиях непрерывного прироста, распределения по многочисленным узлам вычислительной сети, сформировавшихся в конце 2000-х годов, альтернативных традиционным системам управления базами данных и решениям класса Business Intelligence [10].

На сегодняшний день существует множество различных методик применения, в основе которых лежит инструментарий, заимствованный из статистики и математики. Один из таких методов — это A/B testing, который заключается в сравнении контрольной выборки с другими, тем самым находя отклонения. Анализируя его, можно найти причину возникновения, например акт корпоративного мошенничества, тем самым пресечь дальнейшие потери. Например, HSBC использует технологии Больших Данных для противодействия мошеннических операций с пластиковыми картами. С помощью Big Data компания увеличила эффективность службы безопасности в 3 раза, распознавание мошеннических инцидентов — в 10 раз. Экономический эффект от внедрения данных технологий за первые 2 недели превысил 10 млн долл. США. Также на основе анализа Больших Данных в США в сфере здравоохранения компании сократили мошеннические действия в закупке медицинского оборудования, выявляя аномальные тенденции и сравнивая их с общей картиной в отрасли, с \$73 млн к концу 2006 года до всего лишь \$ 40 млн в первом квартале 2007 года [11].

Все больше и больше крупных компаний применяет данную технологию: Coca Cola, Google, VISA, Starbucks, Walmart и другие. Также согласно опубликованному в 2014 году агентством IDC исследованию в 2014 году, объем данного рынка Big Data будет расти примерно на 26,4 % в год и к 2018 году достигнет значения свыше 41,5 миллиардов долларов. США.

Мировое бизнес-сообщество выработало систему «комплаенс» (с англ — compliance), которая позволяет самостоятельно проводить профилактику мошенничества внутри компании. В центре системы «комплаенс» лежит «anti-fraud compliance», которая самостоятельно выявляет, оценивает и отслеживает возможные риски, так называемые «комплаенс-риски», связанные с потенциальными потерями части денежных средств из-за несоответствия

деятельности организации нормативно-правовым документам, как внешним, так и внутренним, которые регулируют деятельность компании. Цель этой системы состоит не только в сведении к минимуму финансового, но и репутационного ущерба, «включая утрату доверия партнеров, инвесторов, клиентов, регулирующих органов, а также в обеспечении для них потока информации именно о добросовестности действий не только самой компании, но и ее персонала» [12].

Еще в 1977 году в США был принят закон о коррупции за рубежом (FCPA), который включал себя пять элементов, раскрывающих суть нарушения данного законодательства, т. е. какая была цель действия, кто является получателем и представителем, в какой форме и с каким намерением. По сути, это первый в мире закон о запрете подкупа иностранных должностных лиц, который предусматривает принятие компаниями различного рода комплаенс программ.

Определенную роль в сфере комплаенс сыграли стандарты управления рисками, основные из которых: COSO ERM 2001 года и Ferma 2002 года. Они послужили толчком для установления основных принципов и концепций внутреннего контроля.

Помимо этого, в апреле 2005 года прошло заседание Базельского комитета по банковскому надзору, где был издан документ «Комплаенс и комплаенс-функция в банках». На тот момент предпринимать серьезные меры было необходимо, так как банки и финансовые институты наиболее подвержены риску мошенничества. Главный результат заключался в том, что были определены основные принципы комплаенса в банках [13].

Помимо Кодекса корпоративного поведения в организации могут быть разработаны: Кодекс корпоративной этики, Политика принятия и дарения подарков, Политика сообщения о нарушениях, Политика о взяточничестве и коррупции, Политика по противодействию легализации доходов, полученных преступным путём, и финансированию терроризма, Политика о конфиденциальности данных, Политика о конфликте интересов.

В российской практике главенствующую роль занимает Федеральный закон о противодействии коррупции № 272-ФЗ от 25 декабря 2008 года, который регулирует сферу противодействия корпоративному мошенничеству в целом, определяя вид, юрисдикции и ответственность при его нарушении, а также органы расследования и подход осуществления.

Важную роль в противодействии корпоративному мошенничеству играет закон от 2010 года «United Kingdom Bribery act», который расширяет действие закона от 1977 года и имеет экстерриториальное юридическое действие. Что касается конвенции ООН по борьбе с коррупцией от 2006 года, каждое государство обязано делать свой вклад в «разработку стандартов и процедур разработке стандартов и процедур, предназначенных для обеспечения добросовестности в работе соответствующих частных организаций, включая кодексы поведения для поощрения использования добросовестной предпринимательской практики в отношениях между коммерческими предприятиями».

Также отдельного внимания заслуживает принятый 30 июля 2002 г. Закон Сарбейнса-Оксли, который представляет собой одно из самых значительных событий по изменению федерального законодательства США по ценным бумагам за последние десятилетия. Закон значительно ужесточает требования к финансовой отчетности и к процессу ее подготовки. Это результат многочисленных корпоративных скандалов, связанных с недобросовестными менеджерами крупных корпораций. Самым известным примером можно назвать историю банкротства Enron. В соответствии с Законом, для акционерных обществ открытого типа: создается новый режим контроля и регулирования финансовой деятельности, происходят существенные изменения в области управления и требований к раскрытию информации.

Помимо приведенных законопроектов также роль играет ряд международных требований, в частности, Конвенция Организации Объединенных Наций против коррупции» от 31.10.2003 г., Конвенция об уголовной ответственности за коррупцию от 27.01.1999 (ETS N 173), Конвенция по борьбе с подкупом иностранных должностных лиц при осуществлении международных коммерческих сделок от 17.12.1997.

### Заключение

Подводя итог, стоит отметить, что проблема корпоративного мошенничества затрагивает компании любых размеров, вследствие чего возрастает роль мероприятий, направленных на противодействие указанному явлению. Одним из самых востребованных методов является комплаенс-контроль. Система комплаенс подразумевает ряд необходимых внутренних документов, главный из которых — это кодекс корпоративного поведения, регламентирующий нормы поведения сотрудников при взаимодействии с клиентами, поставщиками, контрагентами, другими работниками организации и др.

Мошенничество — это проблема, с которой компании могут столкнуться, несмотря на размер, сферу деятельности и страну. Если организация имеет ценное имущество, например деньги, товары и услуги, информацию и т. п., то попытка мошенничества, вероятно, была или будет предпринята. Из-за противоправных действий сотрудников компании фирма разрушается изнутри, при этом претерпевая финансовый ущерб и подрывая имидж компании. При этом малые организации более выражено страдают от корпоративного мошенничества, чем крупные корпорации, в силу менее развитых систем по противодействию мошенничеству. Но важно отметить, что внутри мошеннических схем заложена отлительно высокая интеллектуальная составляющая.

Стоит понимать, что существуют проблемные аспекты, которые нужно учитывать, например: нехватка специалистов, отсутствие основной части инфраструктуры, сложность настройки системы и «незрелость» работы с информацией в целом. Развивающийся на данный момент рынок Big Data очень важен для российских компаний. Но не стоит забывать и про остальные меры безопасности, не теряющие своей актуальности сегодня: налаженная система периодических, плановых, внеплановых и независимых проверок, в частности договоров на приобретение материально-производственных запасов; мониторинг рыночных цен перед осуществлением закупок; создание здоровой корпоративной культуры, создание здоровой корпоративной культуры.

### ЛИТЕРАТУРА

1. Скипин Д.Л. и др. Корпоративное мошенничество: понятие, сущность, риски, влияние на экономическую безопасность // Экономические отношения. — 2019. — Т. 9. — № 3. — С. 2299–2310.
2. Снимщикова И.В., Мельников А.Б., Чугаева Ю.А. Антикоррупционная политика как фактор противодействия корпоративному мошенничеству в нефтяных компаниях // Вестник Северо-Кавказского федерального университета. — 2020. — № 1. — С. 151–157.
3. Телкова Е.А., Чумак Г.В. Мероприятия по выявлению корпоративного мошенничества как угрозы экономической безопасности хозяйствующего субъекта // Бизнес. Образование. Право. — 2018. — № 3. — С. 249–253.

4. Агеева Л.С., Коновалова О.В. Современные подходы к минимизации рисков корпоративного мошенничества в финансовой отчетности // Естественно-гуманитарные исследования. — 2020. — № 2(28). — С. 30–34.
5. Долганов С.И. Общественная опасность корпоративного мошенничества в сфере банковской деятельности // Закон и право. — 2020. — № 11. — С. 136–138.
6. Урошлева А. Корпоративное мошенничество: "слабые места" компаний, методы предотвращения и расследования // Гарант LegalTech. — 2018. — № 3-С. — С. 4–13.
7. Макаренко С.А., Филиппова В.В. Корпоративное мошенничество как угроза экономической безопасности компании // Экономика и предпринимательство. — 2020. — № 11. — С. 763–767.
8. Гулый А.А. Виктимизация юридических лиц-жертв корпоративного мошенничества // Горизонты гуманитарного знания. — 2018. — № 4. — С. 152–158.
9. Ващинкина В.Д., Швырева О.И. Корпоративное мошенничество: способы совершения и ключевые меры противодействия // ББК 65.32 Н34. — 2018. — С. 662.
10. Шумилин П.Е., Нежижимова П.С. Влияние корпоративного мошенничества на бизнес и экономическую безопасность страны в целом // Современные проблемы экономической безопасности, учета и права в Российской Федерации. — 2019. — Т. 2. — С. 5.
11. Zhang J., Wang J., Kong D. Employee treatment and corporate fraud // Economic Modelling. — 2020. — Т. 85. — С. 325–334.
12. Gam Y.K. et al. Evasive shareholder meetings and corporate fraud // Journal of Corporate Finance. — 2021. — Т. 66. — С. 101807.
13. Xiong F., Chapple L., Yin H. The use of social media to detect corporate fraud: A case study approach // Business Horizons. — 2018. — Т. 61. — № 4. — С. 623–633.

**Gladkov Denis Olegovich**

Financial University under the Government of the Russian Federation, Moscow, Russia  
E-mail: D9211121@yandex.ru

**Badma-Khalgaev Ruslan Konstantinovich**

Financial University under the Government of the Russian Federation, Moscow, Russia  
E-mail: tmntgogo@gmail.com

**Sinitsyn Egor Sergeevich**

Financial University under the Government of the Russian Federation, Moscow, Russia  
E-mail: egor.sinitsyn@mail.ru

## Current trends in countering corporate fraud

**Abstract.** This article discusses the issue related to the study of current trends in the field of countering corporate fraud. The author described the key aspects related to the concept of corporate fraud, including the essence of the concept under consideration, its legal characteristics, as well as the place of this phenomenon in the criminal system of Russia.

An important place in this work is reserved for the analysis of activities to counter corporate fraud, and this process is carried out both by the state in the person of individual government institutions, and by the organizations themselves conducting internal audits and other similar activities. The author analyzed the existing legislative framework related to corporate fraud and fraud in the economic sphere, while preserving the principles of historical continuity and the relationship between the laws adopted both within one state and in the process of adopting individual items by other countries. This paper also provides examples of situations in which it is not possible to fully apply methods aimed at countering corporate fraud, while the author identifies two groups as the main reasons, the first of which relates to insufficient elaboration of these methods, and the second group reflects the difficulties that arise from the organizations themselves, on the which are directed by these methods.

In the final part of the work, the author gives recommendations on improving the effectiveness of measures used to counter corporate fraud, as well as on the introduction of new methods that can reduce the negative consequences of the results of individual manifestations of corporate fraud, such as asset appropriation.

**Keywords:** corporate fraud; criminal liability; internal audit; shadow economy; fraud prevention; corruption; Big Data