

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

2025, Том 17, № s2 / 2025, Vol. 17, Iss. s2 <https://esj.today/issue-s2-2025.html>

URL статьи: <https://esj.today/PDF/44FAVN225.pdf>

5.2.3. Региональная и отраслевая экономика (экономические науки)

**Ссылка для цитирования этой статьи:**

Романюк, В. В. Современные стратегии противодействия корпоративному мошенничеству как ключевой элемент экономической безопасности хозяйствующих субъектов / В. В. Романюк // Вестник евразийской науки. — 2025. — Т. 17. — № s2. — URL: <https://esj.today/PDF/44FAVN225.pdf>.

**For citation:**

Romanyuk V.V. Modern strategies for combating corporate fraud as a key element of economic security of business entities. *The Eurasian Scientific Journal*. 2025;17(s2): 44FAVN225. Available at: <https://esj.today/PDF/44FAVN225.pdf>. (In Russ., abstract in Eng.).

УДК 338.14; 338.26; 330.16

**Романюк Виталий Витальевич**

НОЧУ ВО «Московский университет «Синергия», Москва, Россия  
E-mail: [krowel2009@gmail.com](mailto:krowel2009@gmail.com)

*Научный руководитель:* **Калинин Александр Ростиславович**

НОЧУ ВО «Московский университет «Синергия», Москва, Россия  
Профессор кафедры «Оценочной деятельности и корпоративных финансов»  
E-mail: [kalinal@yandex.ru](mailto:kalinal@yandex.ru)

ORCID: <https://orcid.org/0000-0002-1966-5497>

РИНЦ: [https://elibrary.ru/author\\_profile.asp?id=145342](https://elibrary.ru/author_profile.asp?id=145342)

SCOPUS: <https://www.scopus.com/authid/detail.url?authorId=7202840009>

## Современные стратегии противодействия корпоративному мошенничеству как ключевой элемент экономической безопасности хозяйствующих субъектов

**Аннотация.** Исследование посвящено комплексному анализу современных стратегий противодействия корпоративному мошенничеству в контексте обеспечения экономической безопасности хозяйствующих субъектов. В работе представлена концептуальная интерпретация феномена корпоративного мошенничества с акцентом на его системный характер и многогранность проявлений в актуальных экономических условиях. Проведена классификация основных видов корпоративного мошенничества, включая злоупотребления с материальными активами, манипуляции с финансовой отчетностью, коррупционные практики и киберпреступления. Рассмотрены статистические показатели распространенности данного явления: согласно исследованиям, с корпоративным мошенничеством столкнулись более половины компаний в России и странах СНГ, а годовой ущерб от мошеннических действий оценивается в миллиарды рублей. Исследование выявляет ключевые факторы уязвимости хозяйствующих субъектов, среди которых несовершенство систем внутреннего контроля, недостаточный уровень автоматизации бизнес-процессов, отсутствие комплексного подхода к обеспечению экономической безопасности. Обоснована роль комплексных стратегий противодействия корпоративному мошенничеству как фундаментального элемента системы экономической безопасности предприятия. Автором разработана интегрированная модель противодействия корпоративному мошенничеству, включающая организационно-управленческие, нормативно-правовые, технологические и психологические компоненты. В работе детально проанализирован потенциал современных цифровых технологий в сфере противодействия мошенничеству, включая системы DLP (Data Loss Prevention), SIEM (Security Information and

Event Management), технологии поведенческой аналитики (UBA) и искусственного интеллекта. Выявлена взаимосвязь между уровнем цифровой зрелости хозяйствующего субъекта и эффективностью мер по предотвращению корпоративного мошенничества. Определены особенности формирования системы экономической безопасности на различных этапах жизненного цикла организации с учетом эволюции угроз и трансформации механизмов мошеннических действий. Особое внимание уделено принципам построения проактивной системы противодействия, основанной на рискориентированном подходе и предиктивной аналитике. Результаты исследования имеют теоретическую значимость для развития концепции экономической безопасности хозяйствующих субъектов и практическую ценность для разработки эффективных механизмов защиты от корпоративного мошенничества в условиях цифровой трансформации.

**Ключевые слова:** корпоративное мошенничество; экономическая безопасность; внутренний контроль; цифровые технологии; риск-менеджмент; комплаенс; DLP-системы; SIEM-системы; информационная безопасность; антифрод; поведенческая аналитика; экономические преступления; киберугрозы; управление рисками; цифровая трансформация

## Введение

Стремительная цифровизация экономических процессов и глобальные трансформационные изменения в бизнес-среде создают предпосылки для появления новых форм экономических преступлений, среди которых корпоративное мошенничество занимает лидирующие позиции по масштабам наносимого ущерба. Обеспечение экономической безопасности хозяйствующих субъектов в данных условиях выходит за рамки традиционных подходов к защите активов и требует формирования комплексных стратегий, интегрирующих организационно-управленческие, правовые и технологические механизмы противодействия противоправным действиям.

Актуальность темы исследования обусловлена, во-первых, возрастающей сложностью и изощренностью схем корпоративного мошенничества, во-вторых, масштабами экономического ущерба, наносимого хозяйствующим субъектам, в-третьих, необходимостью системного подхода к формированию механизмов экономической безопасности с учетом современных технологических возможностей и трансформации угроз.

Согласно исследованию Аналитического центра НАФИ и компании, «Ингосстрах», в 2023 году с попытками мошенничества столкнулись 91 % россиян, что на 9 процентных пунктов выше показателя 2022 года. При этом количество угроз на одного человека увеличилось с трех до четырех разнообразных схем мошенничества.<sup>1</sup>

По данным Банка России, за 2023 год мошенники похитили у россиян около 15,8 млрд рублей, при этом банки смогли предотвратить мошеннические хищения на сумму 5,8 трлн рублей и отразили 34,77 млн попыток кибермошенников похитить средства у граждан.<sup>2</sup>

Корпоративное мошенничество, будучи многоаспектным явлением, затрагивает не только непосредственные финансовые потери организаций, но и влечет серьезные репутационные риски, подрывает доверие стейкхолдеров, снижает инвестиционную привлекательность и конкурентоспособность. По данным исследования, проведенного

<sup>1</sup> Мошенники стали чаще атаковать россиян. — [Электронный ресурс] Режим доступа: URL: <https://naf1.ru/analyti cs/moshenniki-stali-chashche-atakovat-rossiyan/> (дата обращения 28.04.2025).

<sup>2</sup> Объем похищенных мошенниками средств в 2023 году вырос до 15,8 млрд рублей. — [Электронный ресурс] Режим доступа: URL: <https://www.interfax.ru/russia/945907> (дата обращения 28.04.2025).

экспертами отдела Форензик Группы компаний Б1, среди ключевых факторов, повышающих уязвимость бизнеса к мошенничеству, выделяются несовершенство системы внутреннего контроля (80 %) и недостаточный уровень ее автоматизации (78 %).<sup>3</sup>

В современных условиях научная проблематика противодействия корпоративному мошенничеству характеризуется недостаточной разработанностью системных подходов, интегрирующих организационные, правовые и технологические аспекты обеспечения экономической безопасности хозяйствующих субъектов.

Требуется углубленное исследование взаимосвязи между уровнем цифровой зрелости организации и эффективностью мер по предотвращению мошеннических действий, а также разработка методологических основ формирования проактивных систем защиты.

Объектом исследования выступают экономические и управленческие отношения, возникающие в процессе обеспечения безопасности хозяйствующих субъектов от угроз корпоративного мошенничества.

Предметом исследования являются стратегии, методы и инструменты противодействия корпоративному мошенничеству в системе экономической безопасности хозяйствующих субъектов.

Целью исследования является разработка теоретико-методологических положений и практических рекомендаций по формированию комплексных стратегий противодействия корпоративному мошенничеству в контексте обеспечения экономической безопасности хозяйствующих субъектов.

В соответствии с поставленной целью в работе решаются следующие задачи:

1. Систематизировать теоретические подходы к определению сущности корпоративного мошенничества и его влияния на экономическую безопасность хозяйствующих субъектов.
2. Разработать интегрированную модель противодействия корпоративному мошенничеству с учетом современных технологических возможностей и трансформации угроз.
3. Определить роль и место цифровых технологий в системе противодействия корпоративному мошенничеству и обосновать методологические принципы их внедрения.

Научная новизна исследования заключается в разработке интегрированного подхода к формированию стратегий противодействия корпоративному мошенничеству, основанного на синтезе организационно-управленческих, нормативно-правовых и технологических компонентов в единую систему обеспечения экономической безопасности хозяйствующих субъектов.

Практическая значимость работы определяется возможностью использования разработанных положений и рекомендаций при формировании систем экономической безопасности хозяйствующих субъектов различных организационно-правовых форм и масштабов деятельности, а также при разработке антифрод-систем и внедрении цифровых решений по противодействию корпоративному мошенничеству.

---

<sup>3</sup> Современные тенденции корпоративного мошенничества: анализ причин и методов противодействия. — [Электронный ресурс] Режим доступа: URL: <https://b1.ru/analytics/b1-forensic-trends-review-2025/> (дата обращения 28.04.2025).

## 1. Методы и материалы

Методологическую основу исследования составили общенаучные методы познания, включая анализ, синтез, индукцию, дедукцию, системный и структурно-функциональный подходы. Также были использованы специальные методы исследования: сравнительный анализ, статистический анализ, моделирование, экспертные оценки.

Теоретико-методологическую базу исследования составили труды отечественных и зарубежных авторов в области экономической безопасности, противодействия корпоративному мошенничеству и управления рисками. В их числе научные публикации следующих авторов: Д.О. Гладков, Р.К. Бадма-Халгаев, Е.С. Сеницын [1], А.Л. Кудряшов, Е.А. Кобзев [2], С.С. Юдина [3], Г.З. Альтдинова, С.С. Юдина [4], Е.В. Левкина, Е.Г. Гусев, В.В. Шумихин [5], П.М. Османова, М.З. Валиева [6], Н.В. Капустина [7], А.С. Киселева [8], А.А. Миллер [9], Т.С. Сысоев [10], С.С. Тагаев [11], И.С. Куприянович [12], П.С. Юнг, С.В. Челак [13], Ф.Д. Параскевопуло [14].

Эмпирическую базу исследования составили статистические данные Банка России, материалы исследований Аналитического центра НАФИ, Deloitte Forensic, компании «Ингосстрах», PwC, отчеты аналитических агентств в сфере экономической и информационной безопасности, а также материалы публикаций в профильных изданиях. Информационной базой исследования послужили научные публикации в российских и зарубежных изданиях, материалы научно-практических конференций, аналитические отчеты консалтинговых компаний, данные социологических опросов, нормативно-правовые акты Российской Федерации, регулирующие вопросы противодействия корпоративному мошенничеству и обеспечения экономической безопасности. В процессе сбора, обработки и интерпретации данных использовались следующие методы: контент-анализ; статистический анализ данных о масштабах и динамике корпоративного мошенничества; метод экспертных оценок; моделирование; системный анализ.

## 2. Результаты и обсуждение

Корпоративное мошенничество представляет собой сложный, многоаспектный феномен, характеризующийся высокой адаптивностью к трансформациям экономической среды и способностью к мимикрии под легитимные бизнес-процессы. Методологический фундамент исследования данного явления требует детального рассмотрения его сущностных характеристик, классификационных признаков и механизмов воздействия на экономическую безопасность хозяйствующих субъектов. В настоящее время термин «корпоративное мошенничество» не имеет однозначного закрепления в российском законодательстве, однако отдельные проявления данного феномена регулируются соответствующими нормами Гражданского, Административного и Уголовного кодексов. В научно-методологическом дискурсе сформировалось несколько концептуальных подходов к определению сущности корпоративного мошенничества.

Согласно классификации Ассоциации дипломированных экспертов по мошенничеству (Associated of Certified Fraud Examiners, ACFE), корпоративное мошенничество объединяет злонамеренные, продуманные действия, направленные на хищение чужого имущества или приобретение права на него путем обмана или злоупотребления доверием, которые осуществляются путем использования должностного положения в соответствующей коммерческой организации вопреки интересам собственника и в целях получения личной выгоды.<sup>4</sup>

<sup>4</sup> Корпоративное Мошенничество: Виды, Признаки, Риски, Методы Противодействия. — [Электронный ресурс] Режим доступа: URL: [https://rt-solar.ru/products/solar\\_dozor/blog/2593/](https://rt-solar.ru/products/solar_dozor/blog/2593/) (дата обращения 28.04.2025).

Д.Л. Скипин и Ю.С. Сахно определяют корпоративное мошенничество как фактор дестабилизации экономики страны, который наносит существенный урон экономике предприятий, оцениваемый в 15 % от общей прибыли. Авторы подчеркивают, что именно система риск-менеджмента может предупреждать подобные угрозы, которые в дальнейшем несут негативные экономические последствия для фирмы [15]. Синтезируя различные подходы, можно определить корпоративное мошенничество как комплекс умышленных противоправных действий сотрудников организации или третьих лиц, направленных на присвоение активов компании или создание недостоверной информации финансового и нефинансового характера для получения необоснованных экономических выгод в ущерб интересам хозяйствующего субъекта и его стейкхолдеров. Особенностью современного корпоративного мошенничества является его трансформация под влиянием цифровизации бизнес-процессов, что приводит к появлению новых форм противоправных действий, основанных на использовании информационных технологий. Эволюционируя от примитивных схем хищения материальных ценностей, корпоративное мошенничество приобретает характер сложных многоуровневых конструкций, интегрирующих технологические, финансовые и психологические компоненты.

Для формирования эффективной стратегии противодействия корпоративному мошенничеству необходима детальная классификация его видов. В научной литературе и практике экономической безопасности существуют различные классификационные схемы, основанные на разных критериях. Наиболее распространенной является классификация, предложенная АСФЕ, которая выделяет три основные категории корпоративного мошенничества: незаконное присвоение активов, коррупционные схемы и мошенничество с финансовой отчетностью.

Таблица 1

**Классификация видов корпоративного мошенничества**

Категория	Подвиды	Характеристика
Мошенничество с материальными активами	Хищение денежных средств	Прямое присвоение наличных денег, фиктивные платежи, манипуляции с возвратами
	Хищение товарно-материальных ценностей	Кражи со склада, фиктивное списание, подмена товаров
	Нецелевое использование активов	Использование корпоративных ресурсов в личных целях
Мошенничество с финансовой отчетностью	Искажение доходов	Завышение выручки, фиктивные продажи
	Искажение расходов	Занижение затрат, неправильная капитализация расходов
	Искажение обязательств	Соккрытие задолженности, манипуляции с резервами
Коррупционные практики	«Откаты»	Получение незаконного вознаграждения при выборе поставщиков
	Конфликт интересов	Заключение сделок с аффилированными структурами
	Коммерческий подкуп	Получение вознаграждения за принятие решений в пользу третьих лиц
Информационное мошенничество	Кража конфиденциальных данных	Несанкционированный доступ к коммерческой тайне
	Промышленный шпионаж	Передача конкурентам технологической информации
	Манипуляции с базами данных	Изменение информации в корпоративных системах
Цифровое мошенничество	Киберпреступления	Несанкционированный доступ к IT-системам, создание фиктивных транзакций
	Мошенничество с идентификацией	Использование чужих учетных данных для доступа к системам
	Мошенничество с алгоритмами	Манипулирование автоматизированными системами принятия решений

Составлено автором на основе анализа материалов<sup>5</sup>

<sup>5</sup> Корпоративное Мошенничество: Виды, Признаки, Риски, Методы Противодействия. — [Электронный ресурс] Режим доступа: URL: [https://rt-solar.ru/products/solar\\_dozor/blog/2593/](https://rt-solar.ru/products/solar_dozor/blog/2593/) (дата обращения 28.04.2025).

Корпоративное мошенничество: виды, причины и методы противодействия. — [Электронный ресурс] Режим доступа: URL: [https://focus.kontur.ru/site/news/22039-korporativnoe\\_moshennichestvo\\_po\\_kakim\\_priznakam\\_vyyavit\\_i\\_kak\\_izbezhat](https://focus.kontur.ru/site/news/22039-korporativnoe_moshennichestvo_po_kakim_priznakam_vyyavit_i_kak_izbezhat) (дата обращения 28.04.2025).

Однако данная классификация не учитывает специфику современных цифровых трансформаций и новые формы мошеннических действий, связанные с информационными технологиями. На основе анализа современной практики и научных исследований предлагается расширенная классификация корпоративного мошенничества, учитывающая технологический аспект (табл. 1).

Статистические данные свидетельствуют о значительных масштабах корпоративного мошенничества в российской экономике. По данным исследования Deloitte Forensic, в последние годы с корпоративным мошенничеством столкнулись 55 % компаний, работающих в России и странах СНГ, причем наиболее подверженным риску, оказался крупный бизнес — 73 % жертв мошенников представляли компании с численностью персонала более 1 тыс. сотрудников.<sup>6</sup>

Наиболее подверженными риску корпоративного мошенничества подразделениями компаний являются отделы и департаменты, отвечающие за проведение закупок (71 %), а также маркетинг и продажи (59 %). При этом среди мошеннических схем лидируют так называемые «откаты» (54 % случаев), использование имущества компании сотрудниками в собственных интересах (22 %), хищение активов (11 %), параллельный бизнес, незаконное использование IP-адресов, фальсификация отчетности и искажение показателей (13 % в совокупности).<sup>7</sup>

Экономическая безопасность хозяйствующих субъектов представляет собой динамическое состояние, характеризующееся способностью предприятия противостоять внешним и внутренним угрозам, адаптироваться к изменяющимся условиям и обеспечивать устойчивое функционирование и развитие. В контексте противодействия корпоративному мошенничеству экономическая безопасность выступает как интегральная характеристика, отражающая защищенность экономических интересов компании от противоправных действий сотрудников и третьих лиц.

Современные подходы к определению экономической безопасности предприятия характеризуются двумя основными аспектами: общим, характеризующим системное управление, и специфическим, определяющим возможности выявлять и противодействовать негативным явлениям [16].

Синтез этих аспектов позволяет рассматривать экономическую безопасность как комплексную систему, направленную не только на выявление и предотвращение угроз, но и на формирование устойчивых механизмов функционирования предприятия в условиях неопределенности и рисков.

Корпоративное мошенничество оказывает многостороннее негативное влияние на экономическую безопасность хозяйствующих субъектов, проявляющееся в следующих аспектах:

1. Финансовые потери, включая прямой экономический ущерб от хищений, нецелевого использования ресурсов, коррупционных схем.
2. Репутационные риски, связанные с потерей доверия клиентов, партнеров, инвесторов при выявлении фактов мошенничества.
3. Регуляторные риски, включающие возможные санкции со стороны государственных органов при нарушении требований законодательства в области противодействия коррупции и мошенничеству.

<sup>6</sup> Эксперты Deloitte назвали самые популярные виды мошенничества в компаниях. — [Электронный ресурс] Режим доступа: URL: <https://www.rbc.ru/business/17/02/2021/602bc3979a794731848c5bc9> (дата обращения 28.04.2025).

<sup>7</sup> Корпоративное мошенничество: "слабые места" компаний, методы предотвращения и расследования. — [Электронный ресурс] Режим доступа: URL: <https://www.garant.ru/article/1217829/> (дата обращения 28.04.2025).

4. Операционные риски, связанные со сбоями в бизнес-процессах из-за мошеннических действий сотрудников и ухудшением качества производимых товаров или услуг.
5. Кадровые риски, проявляющиеся в снижении лояльности и мотивации персонала, ухудшении морально-психологического климата в коллективе при обнаружении фактов мошенничества.

Системное противодействие корпоративному мошенничеству в контексте обеспечения экономической безопасности хозяйствующих субъектов предполагает формирование комплексной интегрированной модели, включающей организационно-управленческие, нормативно-правовые, технологические и психологические компоненты. Современный подход к противодействию корпоративному мошенничеству должен базироваться на риск-ориентированной методологии, предполагающей концентрацию ресурсов на наиболее значимых направлениях и объектах контроля. В России переход от всеобъемлющего контроля к дифференцированному с учетом рисков начался несколько лет назад, и риск-ориентированный подход уже зарекомендовал себя как действенный механизм, повышающий эффективность контрольно-надзорной деятельности.<sup>8</sup>

На основе анализа современных практик и подходов предлагается интегрированная модель противодействия корпоративному мошенничеству, включающая четыре взаимосвязанных блока: предотвращение, выявление, расследование и реагирование (рис. 1).



**Рисунок 1.** Интегрированная модель противодействия корпоративному мошенничеству (составлено автором на основе анализа материалов<sup>9</sup>)

<sup>8</sup> Риск-ориентированный подход: приоритет реформы госконтроля. — [Электронный ресурс] Режим доступа: URL: <https://www.garant.ru/article/1406579/> (дата обращения 28.04.2025).

<sup>9</sup> Как противодействовать корпоративному мошенничеству. — [Электронный ресурс] Режим доступа: URL: <https://uprav.ru/blog/kak-protivodeystvovat-korporativnomu-moshennichestvu/> (дата обращения 28.04.2025).

Методы противодействия корпоративному мошенничеству. — [Электронный ресурс] Режим доступа: URL: <https://searchinform.ru/resheniya/biznes-zadachi/preduprezhdenie-moshennichestva/korporativnoe-moshennichestvo/protivodejstvie-korporativnomu-moshennichestvu/metody-protivodejstviya-korporativnomu-moshennichestvu/> (дата обращения 28.04.2025).

Первый блок интегрированной модели — предотвращение — направлен на создание условий, исключающих или минимизирующих возможности совершения мошеннических действий. Ключевыми элементами данного блока являются:

1. Оценка рисков, включающая идентификацию и анализ уязвимостей в бизнес-процессах, должностных функциях и системах контроля. По результатам такой оценки формируется карта рисков корпоративного мошенничества с указанием вероятности их реализации и потенциального ущерба.
2. Политики и процедуры, регламентирующие деятельность сотрудников в сферах с высоким риском мошенничества (закупки, продажи, финансовые операции, взаимодействие с контрагентами). Особое значение имеет антикоррупционная политика, определяющая нетерпимость компании к любым формам коррупции и мошенничества.
3. Обучение персонала, направленное на повышение осведомленности о способах корпоративного мошенничества, методах его выявления и последствиях для компании и самих сотрудников.
4. Этические нормы и корпоративная культура, формирующие нетерпимость к проявлениям мошенничества и коррупции на всех уровнях организации.
5. Технологические средства превенции, включающие системы разграничения прав доступа, двойного контроля операций, автоматизированного мониторинга транзакций и т. д.

Второй блок — выявление — охватывает комплекс мер по обнаружению признаков корпоративного мошенничества. Ключевыми элементами данного блока являются:

1. Внутренний контроль, включающий регулярные проверки, аудит, инвентаризации, анализ отклонений от установленных показателей.
2. DLP-системы (Data Loss Prevention), обеспечивающие контроль информационных потоков и предотвращающие утечку конфиденциальной информации. Современные DLP-решения позволяют не только блокировать несанкционированную передачу данных, но и выявлять подозрительную активность пользователей, свидетельствующую о возможных мошеннических намерениях.
3. SIEM-системы (Security Information and Event Management), собирающие и анализирующие события безопасности из различных источников для выявления аномалий и инцидентов.
4. Поведенческая аналитика (UBA — User Behavior Analytics), основанная на анализе действий пользователей и выявлении отклонений от нормального поведения. Системы UBA применяют алгоритмы машинного обучения для моделирования стандартных паттернов поведения пользователей и идентификации аномалий, которые могут свидетельствовать о мошеннических действиях.<sup>10</sup>
5. Горячие линии и механизмы анонимного информирования, позволяющие сотрудникам сообщать о подозрительных действиях коллег без риска для своей карьеры и репутации.

Третий блок — расследование — включает процедуры по установлению фактов корпоративного мошенничества, их документированию и сбору доказательств.

<sup>10</sup> Anti-malware.ru. Обзор Solar Dozor UBA, модуля поведенческого анализа пользователей. — [Электронный ресурс] Режим доступа: URL: <https://www.anti-malware.ru/reviews/Solar-Dozor-UBA> (дата обращения 28.04.2025).

Ключевыми элементами данного блока являются:

1. Корпоративные расследования, проводимые службой безопасности или внутреннего аудита с использованием специальных методик и инструментов.
2. Форензик (Forensic) — комплекс мероприятий по выявлению и фиксации фактов финансовых злоупотреблений и мошенничества с использованием специальных методик и технологий.
3. Аналитика больших данных, позволяющая выявлять скрытые связи и закономерности в массивах информации, которые могут указывать на мошеннические схемы.
4. Цифровая криминалистика, направленная на поиск, сбор и анализ цифровых доказательств мошенничества (данные с компьютеров, серверов, мобильных устройств, облачных хранилищ).

Четвертый блок — реагирование — охватывает меры по устранению негативных последствий выявленных фактов мошенничества и предотвращению подобных инцидентов в будущем.

Ключевыми элементами данного блока являются:

1. Дисциплинарные меры в отношении виновных лиц, включая увольнение, ограничение полномочий, материальную ответственность.
2. Правовое преследование, включающее взаимодействие с правоохранительными органами для привлечения виновных к административной или уголовной ответственности.
3. Совершенствование системы контроля на основе анализа выявленных инцидентов с целью устранения уязвимостей, которые были использованы мошенниками.
4. Минимизация последствий, включая возмещение ущерба, восстановление деловой репутации, коммуникацию с заинтересованными сторонами.

Эффективность предложенной модели обеспечивается соблюдением ряда принципов:

1. Комплексность и системность — взаимосвязанная реализация всех блоков модели, охватывающих полный цикл противодействия корпоративному мошенничеству.
2. Риск-ориентированность — концентрация ресурсов на направлениях с наиболее высоким риском корпоративного мошенничества и потенциально значительными негативными последствиями.
3. Непрерывность и проактивность — постоянный мониторинг и упреждающее выявление рисков корпоративного мошенничества.
4. Адаптивность — гибкое изменение методов и инструментов противодействия в зависимости от трансформации угроз и условий деятельности компании.
5. Технологичность — использование современных цифровых технологий для автоматизации процессов контроля и аналитики.

Особую роль в современных стратегиях противодействия корпоративному мошенничеству играют цифровые технологии, обеспечивающие автоматизацию процессов контроля, аналитики и предотвращения мошеннических действий.

Анализ современных тенденций в сфере технологического обеспечения экономической безопасности позволяет выделить следующие ключевые технологии, применяемые для противодействия корпоративному мошенничеству:

1. DLP-системы (Data Loss Prevention) — решения для предотвращения утечек конфиденциальной информации, которые контролируют все каналы коммуникации и передачи данных в компании. Современные DLP-решения интегрируют возможности поведенческого анализа, что позволяет выявлять аномалии в действиях пользователей и превентивно блокировать потенциальные утечки информации. Примерами таких систем являются InfoWatch Traffic Monitor, Solar Dozor, Falcongaze SecureTower, SearchInform KIB, Zecurion Zgate.<sup>11</sup>

2. SIEM-системы (Security Information and Event Management) — решения для сбора, нормализации, корреляции и анализа событий безопасности из различных источников. SIEM-системы позволяют выявлять инциденты безопасности, в том числе связанные с мошенническими действиями, путем анализа логов и событий в корпоративных системах. Ключевыми представителями данного класса решений на российском рынке являются MaxPatrol SIEM, R-Vision SIEM, QRadar, UserGate SIEM, Security Vision IRP/SOAR.<sup>12</sup>

3. Системы поведенческой аналитики (UBA/UEBA — User and Entity Behavior Analytics) — решения, анализирующие поведение пользователей и сущностей в информационных системах для выявления аномалий и потенциальных угроз. Данные системы используют алгоритмы машинного обучения для создания профилей нормального поведения пользователей и выявления отклонений, которые могут свидетельствовать о мошеннических действиях. Современные UBA-решения позволяют выявлять такие виды корпоративного мошенничества, как захват аккаунтов, мошенничество с транзакциями, аномальное поведение пользователей.<sup>13</sup>

4. Системы антифрод (Anti-fraud) — специализированные решения для выявления и предотвращения мошенничества в финансовой сфере. Данные системы используют алгоритмы машинного обучения и искусственного интеллекта для анализа транзакций и выявления подозрительных операций. Современные антифрод-системы интегрируют множество источников данных и применяют комплексный подход к оценке рисков мошенничества. Ожидается, что к 2025 году мировой рынок систем противодействия мошенничеству превысит 50 млрд долларов США.<sup>14</sup>

5. Искусственный интеллект и машинное обучение — технологии, применяемые для выявления скрытых закономерностей и аномалий в данных, которые могут свидетельствовать о мошеннических действиях. Алгоритмы машинного обучения используются для создания моделей нормального поведения пользователей и выявления отклонений от них. В 2024 году мошенники активно начали использовать дипфейки для совершения преступлений, а число подобных атак увеличилось более чем на 10 % за год, что вынуждает компании обучать свои антифрод-системы распознавать такие угрозы.<sup>15</sup>

<sup>11</sup> Radiuscompany.ru. DLP Системы. Внедрение DLP систем российского производства. — [Электронный ресурс] Режим доступа: URL: <https://ib.radiuscompany.ru/products-type/predotvrashhenie-utechki-dannyh-dlp/> (дата обращения 28.04.2025).

<sup>12</sup> Anti-malware.ru. SIEM-системы: Современный инструмент для управления кибербезопасностью. — [Электронный ресурс] Режим доступа: URL: <https://sprutmonitor.ru/blog/siem-sistemy/> (дата обращения 28.04.2025).

<sup>13</sup> Habr.com. Как UEBA помогает повышать уровень кибербезопасности. — [Электронный ресурс] Режим доступа: URL: <https://habr.com/ru/company/roi4cio/blog/436082> (дата обращения 28.04.2025).

<sup>14</sup> Bigdataschool.ru. Большие данные и машинное обучение в антифрод-системах. — [Электронный ресурс] Режим доступа: URL: <https://bigdataschool.ru/blog/antifraud-cases.html> (дата обращения 28.04.2025).

<sup>15</sup> РБК Тренды. ИИ против мошенников: как антифрод-системы учатся распознавать угрозы. — [Электронный ресурс] Режим доступа: URL: <https://trends.rbc.ru/trends/industry/67a05f319a79471a124f1732> (дата обращения 28.04.2025).

6. Биометрические технологии — решения, использующие биометрические данные (отпечатки пальцев, распознавание лица, голоса, радужной оболочки глаза) для идентификации и аутентификации пользователей. Данные технологии повышают безопасность за счет использования уникальных физиологических характеристик человека, которые сложно подделать.

7. Блокчейн-технологии — распределенные реестры, обеспечивающие прозрачность и неизменность данных. Применение блокчейна в корпоративных системах позволяет создать неизменяемую запись всех транзакций, что значительно затрудняет манипуляции с данными и подделку документов.

Интеграция перечисленных технологий в единую систему противодействия корпоративному мошенничеству позволяет создать многоуровневую защиту, обеспечивающую комплексный подход к обеспечению экономической безопасности хозяйствующих субъектов.

Важным аспектом применения цифровых технологий в противодействии корпоративному мошенничеству является их интеграция в общую систему управления рисками организации. Риск-ориентированный подход предполагает концентрацию ресурсов на наиболее критичных направлениях и процессах, подверженных риску мошенничества.

На основе анализа статистических данных и исследований в области корпоративного мошенничества, проведенных ведущими консалтинговыми компаниями, можно выделить следующие ключевые зоны риска, требующие особого внимания при построении системы противодействия мошенничеству (табл. 2).

**Таблица 2**

**Зоны риска корпоративного мошенничества**

Зона риска	Типичные схемы мошенничества	Уровень риска
Закупки	«Откаты», завышение цен, фиктивные закупки, манипуляции с тендерной документацией	Высокий (71 % компаний)
Маркетинг и продажи	Фиктивные клиенты, манипуляции с ценами и скидками, неучтенные продажи	Высокий (59 % компаний)
Финансы и бухгалтерия	Подделка финансовой отчетности, фиктивные транзакции, манипуляции с резервами	Средний
ИТ-системы	Несанкционированный доступ к данным, манипуляции с алгоритмами, создание «черных ходов»	Средний
Логистика и склад	Хищение товарно-материальных ценностей, подмена продукции, фиктивное списание	Средний
Управление персоналом	Фиктивные сотрудники, манипуляции с компенсациями и бонусами	Низкий

*Составлено автором на основе анализа материалов<sup>16</sup>*

Согласно исследованию Deloitte Forensic, в странах СНГ корпоративное мошенничество исторически является одной из ключевых угроз для бизнеса, как с точки зрения финансовых, так и репутационных рисков.<sup>17</sup> При этом в последние годы с корпоративным мошенничеством столкнулись более половины (55 %) работающих в России и странах СНГ компаний, причем

<sup>16</sup> РБК. Эксперты Deloitte назвали самые популярные виды мошенничества в компаниях. — [Электронный ресурс] Режим доступа: URL: <https://www.rbc.ru/business/17/02/2021/602bc3979a794731848c5bc9> (дата обращения 28.04.2025).

ГАРАНТ.РУ. Корпоративное мошенничество: «слабые места» компаний, методы предотвращения и расследования. — [Электронный ресурс] Режим доступа: URL: <https://www.garant.ru/article/1217829/> (дата обращения 28.04.2025).

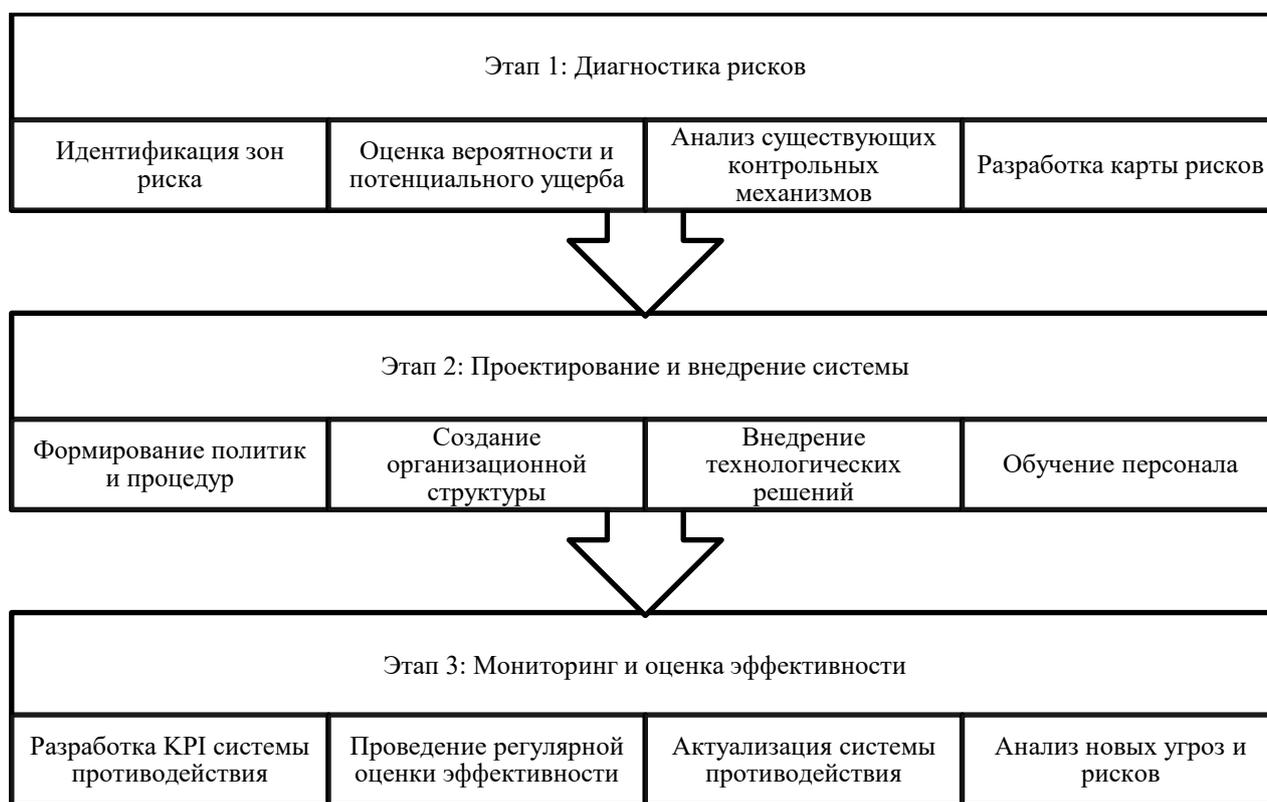
<sup>17</sup> Deloitte. Корпоративное мошенничество. Результаты опроса участников рынка. — [Электронный ресурс] Режим доступа: URL: <https://www2.deloitte.com/ru/ru/pages/finance/articles/2021/corporate-fraud-survey-results.html> (дата обращения 28.04.2025).

наиболее подвержен этому риску оказался крупный бизнес — 73 % жертв мошенников представляли компании с численностью персонала более 1 тыс. человек.

В условиях цифровой трансформации бизнеса особую актуальность приобретает проблема цифрового мошенничества, связанного с использованием современных технологий для совершения противоправных действий. Согласно данным РБК, Тренды, в 2024 году значительно увеличилось количество мошеннических атак с использованием дипфейков и других технологий искусственного интеллекта, что потребовало от компаний пересмотра подходов к обеспечению информационной безопасности и противодействию мошенничеству.

Эффективная стратегия противодействия корпоративному мошенничеству должна учитывать специфику функционирования организации, отраслевые особенности ее деятельности, структуру управления и корпоративную культуру. При этом ключевым принципом построения такой стратегии является комплексность и системность, предполагающие интеграцию организационных, правовых, технологических и психологических мер в единую систему экономической безопасности.

На основе анализа современных подходов и практик противодействия корпоративному мошенничеству, предлагается следующий алгоритм формирования комплексной стратегии противодействия данному феномену (рис. 2).



**Рисунок 2.** Алгоритм формирования комплексной стратегии противодействия корпоративному мошенничеству (составлено автором на основе анализа материалов<sup>18</sup>)

<sup>18</sup> Как противодействовать корпоративному мошенничеству. — [Электронный ресурс] Режим доступа: URL: <https://uprav.ru/blog/kak-protivodeystvovat-korporativnomu-moshennichestvu/> (дата обращения 28.04.2025).

Рекомендации по противодействию корпоративному мошенничеству. — [Электронный ресурс] Режим доступа: URL: <https://searchinform.ru/resheniya/biznes-zadachi/preduprezhdenie-moshennichestva/korporativnoe-moshennichestvo/protivodejstvie-korporativnomu-moshennichestvu/rekomendacii-protivodejstviya-korporativnogo-moshennichestva/> (дата обращения 28.04.2025).

Первый этап — диагностика рисков — направлен на выявление уязвимостей в системе экономической безопасности организации и определение потенциальных угроз корпоративного мошенничества. Диагностика включает следующие ключевые элементы:

1.1. Идентификация зон риска — выявление бизнес-процессов, должностей и операций, наиболее подверженных риску мошенничества. Особое внимание следует уделить процессам закупок, маркетинга и продаж, финансовым операциям, управлению активами.

1.2. Оценка вероятности и потенциального ущерба — экспертная и статистическая оценка вероятности реализации различных схем мошенничества и возможного экономического и репутационного ущерба.

1.3. Анализ существующих контрольных механизмов — оценка эффективности действующих в организации механизмов внутреннего контроля, выявление пробелов и недостатков.

1.4. Разработка карты рисков — визуализация и систематизация выявленных рисков корпоративного мошенничества с учетом их вероятности и потенциального ущерба.

Второй этап — проектирование и внедрение системы противодействия корпоративному мошенничеству — включает следующие элементы:

2.1. Формирование политик и процедур — разработка и внедрение антикоррупционной политики, кодекса этики, процедур управления конфликтом интересов, регламентов ключевых бизнес-процессов с учетом выявленных рисков.

2.2. Создание организационной структуры — формирование системы органов и подразделений, ответственных за противодействие корпоративному мошенничеству, включая службу безопасности, внутренний аудит, комплаенс-службу, комитет по этике.

2.3. Внедрение технологических решений — интеграция современных цифровых технологий (DLP, SIEM, UBA, антифрод-системы) в единую систему противодействия корпоративному мошенничеству.

2.4. Обучение персонала — проведение регулярных тренингов и информационных кампаний, направленных на повышение осведомленности сотрудников о рисках корпоративного мошенничества и методах его предотвращения.

Третий этап — мониторинг и оценка эффективности — направлен на обеспечение постоянного совершенствования системы противодействия корпоративному мошенничеству и включает следующие элементы:

3.1. Разработка KPI системы противодействия — формирование системы ключевых показателей эффективности, позволяющих оценить результативность мер по предотвращению и выявлению корпоративного мошенничества.

3.2. Проведение регулярной оценки эффективности — периодический аудит системы противодействия корпоративному мошенничеству, включающий анализ выявленных инцидентов, оценку работы контрольных механизмов, анализ обратной связи от сотрудников.

3.3. Актуализация системы противодействия — корректировка политик, процедур, организационной структуры и технологических решений с учетом результатов оценки эффективности.

3.4. Анализ новых угроз и рисков — мониторинг изменений внешней и внутренней среды организации, выявление новых потенциальных угроз корпоративного мошенничества и их учет при актуализации системы противодействия.

Реализация предложенного алгоритма позволяет сформировать гибкую и адаптивную систему противодействия корпоративному мошенничеству, учитывающую специфику конкретной организации и способную оперативно реагировать на изменения внешней и внутренней среды.

Особое значение в современных условиях приобретает интеграция цифровых технологий в систему экономической безопасности хозяйствующих субъектов. При этом важно соблюдать баланс между технологическими и организационными мерами противодействия корпоративному мошенничеству, поскольку даже самые современные информационные системы не могут заменить грамотно выстроенные бизнес-процессы и корпоративную культуру.

Перспективным направлением развития систем противодействия корпоративному мошенничеству является применение технологий искусственного интеллекта и машинного обучения для создания самообучающихся антифрод-систем, способных адаптироваться к новым схемам мошенничества. Как отмечается в статье «Антифрод на пороге машинного обучения», классические методы обнаружения мошенничества, используемые в течение длительного времени, становятся менее эффективными, что приводит к необходимости перехода к более продвинутым технологиям на основе искусственного интеллекта.<sup>19</sup>

В условиях глобальной цифровизации и усложнения бизнес-процессов эффективное противодействие корпоративному мошенничеству требует комплексного подхода, объединяющего организационные, правовые и технологические меры в единую систему обеспечения экономической безопасности хозяйствующих субъектов. Разработанная в рамках данного исследования интегрированная модель противодействия корпоративному мошенничеству позволяет учесть многоаспектный характер данного феномена и предложить конкретные инструменты для минимизации рисков и предотвращения негативных последствий для деятельности организаций.

### Выводы

Проведенное исследование современных стратегий противодействия корпоративному мошенничеству как ключевого элемента экономической безопасности хозяйствующих субъектов позволяет сделать следующие выводы.

Во-первых, в результате систематизации теоретических подходов к определению сущности корпоративного мошенничества и его влияния на экономическую безопасность хозяйствующих субъектов установлено, что корпоративное мошенничество представляет собой комплекс умышленных противоправных действий сотрудников организации или третьих лиц, направленных на присвоение активов компании или создание недостоверной информации финансового и нефинансового характера для получения необоснованных экономических выгод в ущерб интересам хозяйствующего субъекта и его стейкхолдеров. Корпоративное мошенничество оказывает многостороннее негативное влияние на экономическую безопасность организаций, проявляющееся в финансовых потерях, репутационных рисках, регуляторных, операционных и кадровых рисках. Согласно статистическим данным, с корпоративным мошенничеством сталкиваются более половины компаний в России и странах СНГ, причем наиболее подверженным риску оказывается крупный бизнес. Наиболее распространенными видами корпоративного мошенничества являются «откаты» (54 % случаев), использование имущества компании сотрудниками в собственных интересах (22 %),

<sup>19</sup> Информационная безопасность решения и рекомендации. Антифрод на пороге машинного обучения. — [Электронный ресурс] Режим доступа: URL: <https://ib-bank.ru/bisjournal/post/498> (дата обращения 28.04.2025).

хищение активов (11 %), а наиболее подверженными риску подразделениями — отделы закупок (71 %) и маркетинга и продаж (59 %).

Во-вторых, разработана интегрированная модель противодействия корпоративному мошенничеству, включающая четыре взаимосвязанных блока: предотвращение, выявление, расследование и реагирование. Модель учитывает современные технологические возможности и трансформацию угроз корпоративного мошенничества в условиях цифровизации бизнес-процессов. Предложен алгоритм формирования комплексной стратегии противодействия корпоративному мошенничеству, включающий три последовательных этапа: диагностику рисков, проектирование и внедрение системы, мониторинг и оценку эффективности. Реализация данного алгоритма позволяет сформировать гибкую и адаптивную систему противодействия корпоративному мошенничеству, учитывающую специфику конкретной организации и способную оперативно реагировать на изменения внешней и внутренней среды.

В-третьих, определена роль и место цифровых технологий в системе противодействия корпоративному мошенничеству и обоснованы методологические принципы их внедрения. Ключевыми технологиями, применяемыми для противодействия корпоративному мошенничеству, являются DLP-системы, SIEM-системы, системы поведенческой аналитики (UBA/UEBA), антифрод-системы, искусственный интеллект и машинное обучение, биометрические технологии, блокчейн-технологии. Интеграция данных технологий в единую систему противодействия корпоративному мошенничеству позволяет создать многоуровневую защиту, обеспечивающую комплексный подход к обеспечению экономической безопасности хозяйствующих субъектов. При этом важно соблюдать баланс между технологическими и организационными мерами противодействия корпоративному мошенничеству, поскольку даже самые современные информационные системы не могут заменить грамотно выстроенные бизнес-процессы и корпоративную культуру.

Таким образом, эффективное противодействие корпоративному мошенничеству в современных условиях требует комплексного подхода, объединяющего организационные, правовые и технологические меры в единую систему обеспечения экономической безопасности хозяйствующих субъектов. Предложенная в рамках данного исследования интегрированная модель противодействия корпоративному мошенничеству позволяет учесть многоаспектный характер данного феномена и предложить конкретные инструменты для минимизации рисков и предотвращения негативных последствий для деятельности организаций.

## ЛИТЕРАТУРА

1. 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. — EDN FROFMP.
2. Кудряшов, А.Л. Перспективные мероприятия в области минимизации рисков корпоративного мошенничества / А.Л. Кудряшов, Е.А. Кобзев // Вестник евразийской науки. — 2023. — Т. 15, № S1. — EDN SINIXA.
3. Юдина, С.С. Корпоративные мошенничества: методы предотвращения / С.С. Юдина — DOI 10.24412/2500-1000-2023-1-3-160-163. // Международный журнал гуманитарных и естественных наук. — 2023. — № 1-3(76). — С. 160–163 — EDN EQENQX.
4. Альтдинова, Г.З. Современные подходы к минимизации рисков корпоративного мошенничества с финансовой отчетностью / Г.З. Альтдинова, С.С. Юдина — DOI 10.18334/err.13.2.117116. // Экономика, предпринимательство и право. — 2023. — Т. 13, № 2. — С. 577–586 — EDN HTUXTR.

5. Левкина, Е.В. Корпоративное мошенничество как угроза экономической безопасности предприятия / Е.В. Левкина, Е.Г. Гусев, В.В. Шумихин // Финансовый менеджмент. — 2024. — № 7. — С. 71–79. — EDN ZLICUH.
6. Османова, П.М. Корпоративное мошенничество: практика выявления и противодействия / П.М. Османова, М.З. Валиева // Экономика и безопасность. — 2024. — № 2. — С. 64–69. — EDN BYFKJA.
7. Капустина, Н.В. Корпоративное мошенничество как угроза экономической безопасности организации / Н.В. Капустина // Вестник евразийской науки. — 2024. — Т. 16, № S1. — EDN JZOFJR.
8. Киселева, А.С. Противодействие корпоративному мошенничеству в целях обеспечения экономической безопасности предприятия / А.С. Киселева // Интернаука. — 2024. — № 22-3(339). — С. 36–37. — EDN INVRAD.
9. Миллер, А.А. Корпоративное мошенничество: правовые проблемы определения и противодействия / А.А. Миллер // Вестник науки. — 2024. — Т. 1, № 7(76). — С. 241–248. — EDN OLQZWM.
10. Сысоев, Т.С. Нормативно-правовые основы противодействия корпоративному мошенничеству и коррупции в РФ / Т.С. Сысоев — DOI 10.37539/2949-1991.2023.9.9.027. // Флагман науки. — 2023. — № 9(9). — С. 673–675 — EDN MYLBAR.
11. Тагаев, С.С. Внутренний аудит и контроль корпоративного мошенничества / С.С. Тагаев // Научный аспект. — 2024. — Т. 11, № 1. — С. 1321–1325. — EDN VFAZVZ.
12. Куприянович, И.С. Роль внутреннего контроля в предупреждении корпоративного мошенничества / И.С. Куприянович // Флагман науки. — 2024. — № 1(12). — С. 379–381. — EDN JSBWDT.
13. Юнг, П.С. Корпоративные мошенничества как угроза экономической безопасности хозяйствующих субъектов / П.С. Юнг, С.В. Челак // Здоровье — основа человеческого потенциала: проблемы и пути их решения. — 2023. — Т. 18, № 3. — С. 989–992. — EDN QGEWDA.
14. Параскевопуло, Ф.Д. Корпоративное мошенничество: виды и этапы расследований / Ф.Д. Параскевопуло // Научный аспект. — 2024. — Т. 8, № 2. — С. 961–968. — EDN CFAJGV.
15. Корпоративное мошенничество: понятие, сущность, риски, влияние на экономическую безопасность / Д.Л. Скипин, Ю.С. Сахно, Л.А. Баденова, М.О. Кузнецов — DOI 10.18334/eo.9.3.41049. // Экономические отношения. — 2019. — Т. 9, № 3. — С. 2299–2310 — EDN НТΥΚΙΟ.
16. Ревина, Е.В. Подходы к определению экономической безопасности предприятия / Е.В. Ревина // Бенефициар. — 2023. — № 123. — С. 3–5. — EDN JYZUNZ.

**Romanyuk Vitaly Vitalievich**

Moscow University «Synergy», Moscow, Russia  
E-mail: [krowel2009@gmail.com](mailto:krowel2009@gmail.com)

*Academic adviser:* **Kalinin Alexander Rostislavovich**

Moscow University «Synergy», Moscow, Russia  
E-mail: [kalinal@yandex.ru](mailto:kalinal@yandex.ru)

ORCID: <https://orcid.org/0000-0002-1966-5497>

RSCI: [https://elibrary.ru/author\\_profile.asp?id=145342](https://elibrary.ru/author_profile.asp?id=145342)

SCOPUS: <https://www.scopus.com/authid/detail.url?authorId=7202840009>

## **Modern strategies for combating corporate fraud as a key element of economic security of business entities**

**Abstract.** The study is devoted to a comprehensive analysis of modern strategies for combating corporate fraud in the context of ensuring the economic security of business entities. The paper presents a conceptual interpretation of the corporate fraud phenomenon with an emphasis on its systemic nature and multifaceted manifestations in the current economic conditions. The main types of corporate fraud are classified, including abuse of tangible assets, manipulation of financial statements, corrupt practices and cybercrime. Statistical indicators of the prevalence of this phenomenon are considered: according to research, more than half of companies in Russia and the CIS countries have encountered corporate fraud, and the annual damage from fraudulent activities is estimated at billions of rubles. The study identifies key vulnerability factors for business entities, including imperfect internal control systems, insufficient automation of business processes, and the lack of a comprehensive approach to ensuring economic security. The role of comprehensive strategies for countering corporate fraud as a fundamental element of the enterprise economic security system is substantiated. The author has developed an integrated model for countering corporate fraud, including organizational and managerial, regulatory, technological and psychological components. The paper provides a detailed analysis of the potential of modern digital technologies in the field of counteracting fraud, including DLP (Data Loss Prevention), SIEM (Security Information and Event Management), behavioral analytics (UBA) and artificial intelligence. The relationship between the level of digital maturity of an economic entity and the effectiveness of measures to prevent corporate fraud is revealed. The features of the formation of an economic security system at various stages of the organization's life cycle are determined, taking into account the evolution of threats and the transformation of fraudulent mechanisms. Particular attention is paid to the principles of building a proactive counteraction system based on a risk-oriented approach and predictive analytics. The results of the study are of theoretical significance for the development of the concept of economic security of economic entities and practical value for the development of effective mechanisms for protecting against corporate fraud in the context of digital transformation.

**Keywords:** corporate fraud; economic security; internal control; digital technologies; risk management; compliance; DLP systems; SIEM systems; information security; antifraud; behavioral analytics; economic crimes; cyber threats; digital transformation