

Интернет-журнал «Отходы и ресурсы» <https://resources.today>
Russian Journal of Resources, Conservation and Recycling

2025, Том 12, № s1 / 2025, Vol. 12, Iss. s1 <https://resources.today/issue-s1-2025.html>

URL статьи: <https://resources.today/PDF/14FAOR125.pdf>

DOI: 10.15862/14FAOR125 (<https://doi.org/10.15862/14FAOR125>)

5.2.3. Региональная и отраслевая экономика (экономические науки)

Ссылка для цитирования этой статьи:

Бирюков, В. В. Организационно-методические основы создания корпоративных горячих линий по противодействию мошенничеству на основе международного опыта / В. В. Бирюков // Отходы и ресурсы. — 2025. — Т. 12. — № s1. — URL: <https://resources.today/PDF/14FAOR125.pdf>. DOI: 10.15862/14FAOR125.

For citation:

Biryukov V.V. Organizational and methodological foundations for creating corporate hotlines to combat fraud based on international experience. *Russian Journal of Resources, Conservation and Recycling*. 2025; 12(s1): 14FAOR125. Available at: <https://resources.today/PDF/14FAOR125.pdf>. DOI: 10.15862/14FAOR125. (In Russ., abstract in Eng.).

УДК 334.7:34

Бирюков Вячеслав Витальевич

ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
E-mail: birslava2004@mail.ru

ORCID: <https://orcid.org/0009-0000-2010-1923>

Организационно-методические основы создания корпоративных горячих линий по противодействию мошенничеству на основе международного опыта

Аннотация. Современная экономическая среда характеризуется возрастающими рисками корпоративного мошенничества, требующими от организаций разработки эффективных механизмов противодействия, среди которых особое значение приобретают корпоративные горячие линии как инструмент раннего выявления и предотвращения финансовых нарушений. Данное исследование представляет комплексный анализ международного опыта создания и функционирования корпоративных систем сообщения о мошенничестве, включающий изучение нормативно-правовой базы ведущих юрисдикций, методологических подходов к организации внутрикорпоративных каналов связи и технологических решений для обеспечения эффективности детекции правонарушений. Исследование охватывает анализ эволюции концептуальных подходов от классических моделей внутреннего контроля до современных интегрированных систем управления рисками, учитывающих специфику цифровой трансформации и изменившиеся требования регуляторов. Особое внимание уделяется сравнительному анализу американской модели, основанной на требованиях Закона Сарбейнса-Оксли, европейского подхода, регламентированного Директивой ЕС о защите лиц, сообщающих о нарушениях законодательства Союза, и формирующихся практик в юрисдикциях Азиатско-Тихоокеанского региона. Проведённый анализ статистических данных Ассоциации сертифицированных экспертов по борьбе с мошенничеством за 2024 год демонстрирует, что сообщения через внутренние каналы остаются наиболее эффективным способом выявления корпоративного мошенничества, составляя 43 % всех случаев обнаружения, при медианных потерях организаций в размере 1,662 миллиона долларов США на каждый случай. Результаты исследования свидетельствуют о необходимости перехода от традиционных телефонных горячих линий к мультиканальным цифровым платформам, интегрирующим веб-формы, мобильные приложения и средства искусственного интеллекта для анализа поступающих сообщений. Разработанная концептуальная модель организационно-

методических основ включает шесть ключевых компонентов: нормативно-правовое обеспечение, организационную структуру, технологическую инфраструктуру, процедуры обработки сообщений, систему защиты информаторов и механизмы мониторинга эффективности.

Ключевые слова: корпоративные горячие линии; противодействие мошенничеству; внутренний контроль; управление рисками; международные стандарты; цифровая трансформация; корпоративное управление; защита информаторов; финансовые нарушения

Введение

Масштабы корпоративного мошенничества в современной глобальной экономике достигли критических показателей, согласно данным исследования Ассоциации сертифицированных экспертов по борьбе с мошенничеством (ACFE) за 2024 год, организации ежегодно теряют приблизительно 5 % от валовой выручки вследствие различных форм внутренних злоупотреблений.¹ Совокупные потери от 1,921 случая профессионального мошенничества, исследованных в 138 странах и территориях, превысили 3,1 миллиарда долларов США, что эквивалентно среднему ущербу 1,662 миллиона долларов на каждый выявленный случай.²

Актуальность темы исследования обусловлена растущими требованиями регуляторных органов к созданию эффективных механизмов внутреннего контроля, что нашло отражение в принятии Европейским Союзом Директивы 2019/1937 о защите лиц, сообщающих о нарушениях законодательства Союза, которая обязывает организации с численностью более 50 сотрудников создавать внутренние каналы сообщения о правонарушениях.³ Аналогичные тенденции наблюдаются в других юрисдикциях, включая усиление требований Закона Сарбейнса-Оксли в США и разработку национальных стандартов защиты информаторов в странах Азиатско-Тихоокеанского региона.⁴

Научная проблема заключается в отсутствии систематизированного подхода к проектированию корпоративных горячих линий, учитывающего специфику различных юрисдикций, отраслевые особенности и технологические возможности цифровой эпохи. Несмотря на доказанную эффективность внутренних каналов сообщения — они обеспечивают выявление 43 % случаев мошенничества согласно статистике ACFE, что превышает результативность внутреннего аудита в три раза — многие организации продолжают использовать устаревшие подходы, не учитывающие современные требования к конфиденциальности, анонимности и оперативности обработки сообщений.

Объектом исследования выступают организационно-экономические отношения, возникающие в процессе создания и функционирования корпоративных систем противодействия мошенничеству посредством внутренних каналов сообщения о правонарушениях.

Предметом исследования являются методологические подходы, технологические решения и организационные механизмы, обеспечивающие эффективность корпоративных

¹ ACFE Report to the Nations. 2024 Global Fraud Study. [Электронный ресурс]. — URL: <https://legacy.acfe.com/report-to-the-nations/2024/> (дата обращения: 27.01.2025).

² Occupational Fraud 2024: A Report to the Nations. [Электронный ресурс]. — URL: <https://www.acfe.com/-/media/files/acfe/pdfs/rtnn/2024/2024-report-to-the-nations.pdf> (дата обращения: 27.01.2025).

³ EU Whistleblowing Directive Legislation — Safecall Ltd. [Электронный ресурс]. — URL: <https://www.safecall.co.uk/eu-whistleblowing-directive-legislation/> (дата обращения: 27.01.2025).

⁴ Going Public in 2024? Don't Forget Your SOX Whistleblowing Obligation. [Электронный ресурс]. — URL: <https://www.starcompliance.com/going-public-in-2024-dont-forget-your-sox-whistleblowing-obligation/> (дата обращения: 27.01.2025).

горячих линий как инструмента управления рисками мошенничества в условиях различных регуляторных сред и отраслевых контекстов.

Цель исследования — разработка концептуальной модели организационно-методических основ создания корпоративных горячих линий по противодействию мошенничеству на основе анализа международного опыта и современных технологических решений.

Задачи исследования:

1. Провести сравнительный анализ нормативно-правовых подходов к регулированию корпоративных каналов сообщения о правонарушениях в ведущих юрисдикциях мира.
2. Исследовать эволюцию технологических решений и методологических подходов к организации корпоративных горячих линий в контексте цифровой трансформации.
3. Обосновать принципы интегрированной модели создания эффективных систем внутрикорпоративного сообщения о мошенничестве с учётом международных стандартов и лучших практик.

Научная новизна исследования заключается в разработке комплексной концептуальной модели, интегрирующей международные регуляторные требования, технологические инновации и организационные практики в единую методологическую основу для создания эффективных корпоративных систем противодействия мошенничеству. Впервые предложен систематизированный подход к оценке соответствия корпоративных горячих линий требованиям различных юрисдикций с учётом специфики цифровых каналов коммуникации и современных стандартов защиты информации.

Практическая значимость работы определяется возможностью применения разработанных методологических принципов при проектировании корпоративных систем управления рисками мошенничества, что позволит организациям повысить эффективность внутреннего контроля, обеспечить соответствие регуляторным требованиям и минимизировать финансовые потери от внутренних злоупотреблений.

1. Методы и материалы

Методологическую основу исследования составляют принципы системного анализа в области корпоративного управления, позволяющие рассматривать корпоративные горячие линии как интегрированные элементы систем управления рисками

Теоретической базой выступают концепции современного риск-менеджмента, международные стандарты корпоративного управления, включая рекомендации Организации экономического сотрудничества и развития (ОЭСР) по корпоративному управлению и принципы Базельского комитета по банковскому надзору в области операционных рисков.

Особое внимание уделено работам следующих авторов: М.Е. Басова [1], Н.Е. Губар [2], М.И. Елаев [3], Д.Г. Заброда, А.В. Капранов [4], Н.А. Кабанова, Д.Д. Накостик [5], Б.Э. Садыржанов [6], Н.С. Семенов [7], И.В. Снимщикова, А.Б. Мельников, Ю.А. Чугаева [8], А.И. Сотов [9], С.К. Сулейманов [10], Г.В. Чумак, А.Е. Суглобов, Е.А. Телкова [11], Н.А. Южакова [12].

В качестве основного метода исследования использован сравнительный анализ международных практик, включающий систематизацию и обобщение регуляторных требований, технологических решений и организационных подходов к созданию корпоративных каналов сообщения о правонарушениях. Применялись методы контент-анализа

нормативных документов, статистического анализа данных исследований ACFE, PwC Global Economic Crime Survey и NAVEX Whistleblowing Benchmark Report, а также методы моделирования интегративных систем управления рисками. Эмпирическую базу исследования составили данные официальные документы международных организаций, национальных регуляторов, исследовательских центров и консалтинговых компаний за период 2023–2025 годов.

2. Результаты и обсуждения

Фундаментальные исследования в области корпоративного управления рисками мошенничества имеют богатую историю развития, начиная с классических работ по теории агентских отношений и асимметрии информации, заложивших основы понимания конфликтов интересов в корпоративных структурах. Эволюция концептуальных подходов к созданию систем внутреннего контроля демонстрирует постепенное усложнение методологического аппарата и расширение инструментария управления рисками, при чём каждый этап развития привносил качественно новые решения в понимание природы корпоративных злоупотреблений и способов их предотвращения.

Американская модель корпоративного контроля, сформировавшаяся под влиянием Закона Сарбейнса-Оксли 2002 года, установила революционные требования к созданию независимых каналов сообщения о финансовых нарушениях. Согласно статистическим данным NAVEX за 2024 год, организации в США демонстрировали медианный показатель 1,78 сообщений на 100 сотрудников, что значительно превышает аналогичные показатели в других регионах.⁵ При этом уровень анонимных сообщений в США составлял 51 %, что существенно ниже европейских показателей (65 %), что свидетельствует о различиях в корпоративной культуре и уровне доверия к системам защиты информаторов.⁶ Как видно из таблицы 1, эволюция подходов к корпоративному контролю характеризуется переходом от реактивных к проактивным методам, интеграцией технологических решений и усилением фокуса на защите информаторов.

Таблица 1

Эволюция подходов к корпоративному контролю и противодействию мошенничеству

Период	Регуляторная основа	Ключевые характеристики	Технологические решения	Показатели эффективности
1980–2000 гг.	Саморегулирование отрасли	Внутренний аудит, этические кодексы	Телефонные горячие линии	Низкая детекция (< 20 %)
2002–2010 гг.	Sarbanes-Oxley Act (США)	Обязательные каналы сообщения	Email, веб-формы	Средняя детекция (25–35 %)
2010–2020 гг.	UK Bribery Act, FCPA усиление	Глобальные стандарты	Мобильные приложения	Высокая детекция (35–40 %)
2020 — н.в.	EU Whistleblower Directive	Цифровая интеграция, ИИ	Мультиканальные платформы	Очень высокая (40–45 %)

Составлено автором на основе анализа материалов⁷

⁵ 2025 United States Whistleblowing Benchmarking Statistics. [Электронный ресурс]. — URL: <https://www.navex.com/en-us/northstar/united-states-whistleblowing-statistics/> (дата обращения: 27.01.2025).

⁶ 2025 Regional Whistleblowing Statistics & Benchmarks. [Электронный ресурс]. — URL: <https://www.navex.com/en-us/northstar/regional-whistleblowing-statistics/> (дата обращения: 27.01.2025).

⁷ ACFE Report to the Nations. 2024 Global Fraud Study. [Электронный ресурс]. — URL: <https://legacy.acfe.com/report-to-the-nations/2024/> (дата обращения: 27.01.2025).

2025 Whistleblowing Statistics & Benchmarking. [Электронный ресурс]. — URL: <https://www.navex.com/en-us/northstar/whistleblowing-statistics-benchmark-report/> (дата обращения: 27.01.2025).

Европейская модель, основанная на Директиве ЕС 2019/1937, представляет собой более комплексный подход к защите лиц, сообщающих о нарушениях. Директива требует от организаций с численностью более 50 сотрудников создания внутренних каналов сообщения, обеспечивающих конфиденциальность и защиту от преследований.⁸ Ключевым отличием европейского подхода является акцент на многоуровневой системе защиты: внутренние каналы, обращения к регуляторам и, в исключительных случаях, публичное раскрытие информации.⁹

Международный стандарт ISO 37002:2021 «Системы управления информированием о нарушениях — Руководство» представляет собой глобальную методологическую основу для создания эффективных систем внутрикорпоративного сообщения. Стандарт основан на трёх ключевых принципах: доверие, беспристрастность и защита, реализуемых через четыре основных процесса: получение сообщений, оценка сообщений, реагирование на сообщения и завершение расследований.¹⁰ Важной особенностью стандарта является его универсальность — применимость к организациям любого размера и сферы деятельности, что делает его ценным инструментом для глобальных корпораций.¹¹

Статистический анализ эффективности различных каналов детекции мошенничества, представленный в таблице 2, демонстрирует безусловное лидерство внутренних сообщений среди всех методов выявления корпоративных злоупотреблений.

Таблица 2

**Сравнительная эффективность методов
выявления корпоративного мошенничества (2024 год)**

Метод выявления	Доля обнаружения (%)	Медианные потери (тыс. USD)	Время до обнаружения (мес.)	Региональные различия
Внутренние сообщения	43	120	12	США: 45 %, ЕС: 47 %, АРАС: 41 %
Внутренний аудит	15	150	18	Развитые рынки: выше
Корпоративная безопасность	12	180	15	Крупные организации
Внешний аудит	8	200	24	Публичные компании
Случайное обнаружение	7	250	36	Универсально
Мониторинг документов	5	100	6	Финансовый сектор

Составлено автором на основе анализа материалов¹²

Российская практика создания корпоративных каналов противодействия мошенничеству развивается в контексте общих тенденций совершенствования корпоративного управления и усиления требований к прозрачности деятельности организаций. Крупные российские компании, такие как ПАО «Газпром», Государственная корпорация «Ростех» и другие, активно внедряют системы «горячих линий» по вопросам противодействия мошенничеству, коррупции

⁸ EU Whistleblowing Directive requirements. [Электронный ресурс]. — URL: <https://www.faceup.com/en/eu-whistleblowing-directive> (дата обращения: 27.01.2025).

⁹ The EU Whistleblowing Directive: Progress, Trends, and Expectations for 2024. [Электронный ресурс]. — URL: <https://www.mofo.com/resources/insights/240313-the-eu-whistleblowing-directive-progress-trends> (дата обращения: 27.01.2025).

¹⁰ ISO 37002:2021 — Whistleblowing management systems — Guidelines. [Электронный ресурс]. — URL: <https://www.iso.org/standard/65035.html> (дата обращения: 27.01.2025).

¹¹ ISO 37002 whistleblowing standard — what organisations need to know. [Электронный ресурс]. — URL: <https://www.integrityline.com/expertise/blog/iso-37002/> (дата обращения: 27.01.2025).

¹² Digest the Occupational Fraud Report 2024. [Электронный ресурс]. — URL: <https://www.counterfraud.gov.au/news/general-news/digest-occupational-fraud-report-2024> (дата обращения: 27.01.2025).

и хищениям. Особенностью российского подхода является интеграция антикоррупционных требований с общими принципами противодействия мошенничеству, что отражает специфику национального законодательства в области противодействия коррупции.¹³ Технологическая эволюция корпоративных горячих линий характеризуется переходом от традиционных телефонных систем к интегрированным цифровым платформам. Согласно данным NAVEX Global, впервые в истории веб-отчёты (33,4 %) превзошли телефонные сообщения (29,4 %) по частоте использования, что свидетельствует о предпочтениях пользователей в пользу более удобных и анонимных цифровых каналов. Текстовые сообщения набирают популярность и составляют уже 3 % от общего объёма сообщений, что указывает на важность адаптации систем к изменяющимся коммуникационным предпочтениям.¹⁴ Результаты исследования PwC Global Economic Crime Survey 2024 подтверждают растущую сложность корпоративного мошенничества: киберпреступность стала наиболее распространённой формой экономических преступлений с показателем 44 %, а наиболее разрушительной её считают 40 % респондентов.¹⁵ В странах Центральной и Восточной Европы 75 % руководителей отмечают, что мошенничество в сфере закупок является широко распространённой проблемой, при этом большинство компаний используют аналитику данных для выявления мошенничества.¹⁶ Как показано на рисунке 1, современная архитектура корпоративных систем противодействия мошенничеству представляет собой сложную многоуровневую структуру, интегрирующую различные каналы поступления информации, системы обработки и анализа данных, а также механизмы обратной связи и защиты информаторов.

Анализ региональных различий в функционировании корпоративных горячих линий, представленный в таблице 3, выявляет значительную вариативность в подходах к организации внутренних каналов сообщения в зависимости от культурных, правовых и экономических факторов.

Таблица 3

**Региональные особенности
функционирования корпоративных горячих линий (2024 год)**

Регион	Сообщений на 100 сотр.	Анонимность (%)	Подтверждение (%)	Время расследования (дни)	Основные категории нарушений
Северная Америка	1,75	52	45	65	Рабочее поведение, финансы
Европа	0,67	65	47	85	Коррупция, рабочее поведение
Азиатско-Тихоокеанский	0,78	67	41	75	Финансы, кибербезопасность
Южная Америка	2,97	59	48	95	Коррупция, мошенничество

Составлено автором на основе анализа материалов¹⁷

¹³ Ростех — Горячая линия. [Электронный ресурс]. — URL: <https://rostec.ru/anticorruption/feedback/> (дата обращения: 27.01.2025).

¹⁴ 2025 Whistleblowing Statistics & Benchmarking. [Электронный ресурс]. — URL: <https://www.navex.com/en-us/northstar/whistleblowing-statistics-benchmark-report/> (дата обращения: 27.01.2025).

¹⁵ Global Economic Crime Survey 2024. [Электронный ресурс]. — URL: <https://www.pwc.com/gx/en/services/forensic/s/economic-crime-survey.html> (дата обращения: 27.01.2025).

¹⁶ Global Economic Crime Survey 2024. [Электронный ресурс]. — URL: <https://cee.pwc.com/global-economic-crime-survey-2024-cee-findings.html> (дата обращения: 27.01.2025).

¹⁷ 2025 Regional Whistleblowing Statistics & Benchmarks. [Электронный ресурс]. — URL: <https://www.navex.com/en-us/northstar/regional-whistleblowing-statistics/> (дата обращения: 27.01.2025).

2025 United Kingdom Whistleblowing Benchmarking Statistics. [Электронный ресурс]. — URL: <https://www.navex.com/en-gb/northstar/united-kingdom-whistleblowing-statistics/> (дата обращения: 27.01.2025).

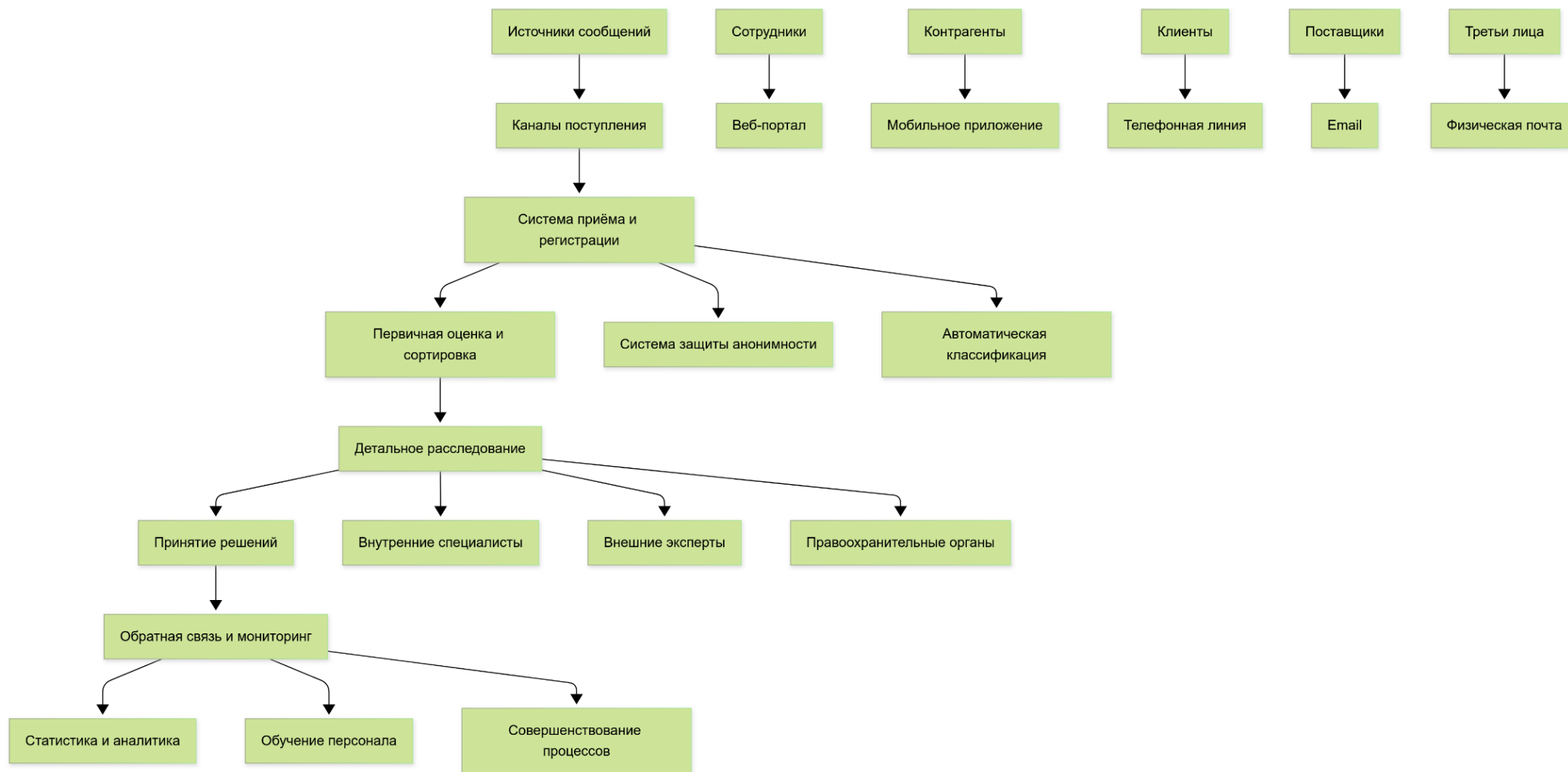


Рисунок 1. Архитектура интегрированной системы корпоративного противодействия мошенничеству (разработано автором)

Ключевым фактором успешности корпоративных систем противодействия мошенничеству является обеспечение доверия сотрудников к процессу сообщения о нарушениях. Исследование NAVEX показывает, что только 51 % компаний в США имеют политику защиты от преследований как часть программы внутренней отчётности, при этом в европейских странах показатели ещё ниже: 27 % во Франции, 36 % в Великобритании и 41 % в Германии.¹⁸

Данная статистика свидетельствует о существенных пробелах в создании культуры открытости и доверия, необходимой для эффективного функционирования систем внутреннего контроля.

Технологические инновации в области корпоративных горячих линий включают использование искусственного интеллекта для автоматической классификации сообщений, блокчейн-технологий для обеспечения неизменности записей и продвинутой аналитики для выявления паттернов мошенничества. Мобильные приложения становятся важным каналом для молодого поколения сотрудников, предпочитающих интуитивно понятные интерфейсы и возможность отправки сообщений в любое время.¹⁹

Обеспечение соответствия требованиям различных юрисдикций требует создания гибких систем, способных адаптироваться к местным особенностям законодательства при сохранении глобальной согласованности процессов. Таблица 4 демонстрирует ключевые требования основных регуляторных режимов к корпоративным системам сообщения о нарушениях.

Таблица 4

Сравнительный анализ регуляторных требований к корпоративным горячим линиям

Юрисдикция	Применимость	Обязательные каналы	Временные рамки	Защита информаторов	Штрафы за несоблюдение
США (SOX)	Публичные компании	Аудиторский комитет	Немедленно	Уголовная ответственность	До 10 лет тюрьмы
ЕС (Директива 2019/1937)	> 50 сотрудников	Письменные/устные	7 дней подтверждение	Запрет преследований	До 200,000 EUR
Великобритания	Листинговые компании	Рекомендованы	Разумные сроки	Трудовое законодательство	Репутационные
ISO 37002	Добровольно	Множественные	Определяется организацией	Принцип защиты	Не применимо

Составлено автором на основе анализа материалов²⁰

Российские организации адаптируют международный опыт с учётом специфики национального законодательства и корпоративной культуры. Согласно исследованиям в области корпоративных коммуникаций, российские компании всё больше внимания уделяют созданию открытых линий коммуникации между руководством и сотрудниками, что способствует формированию атмосферы прозрачности.²¹ Важным трендом является

¹⁸ Whistleblower Hotline Success, in the EU and Beyond. [Электронный ресурс]. — URL: <https://www.navex.com/en-us/blog/article/whistleblower-hotline-success-in-the-eu-and-beyond/> (дата обращения: 27.01.2025).

¹⁹ How to Comply with the EU Whistleblowing Directive. [Электронный ресурс]. — URL: <https://www.corporatecomplianceinsights.com/eu-whistleblower-directive-details/> (дата обращения: 27.01.2025).

²⁰ EU Whistleblowing Directive. The Facts You Need to Know. [Электронный ресурс]. — URL: <https://www.taylorwessing.com/en/insights-and-events/insights/whistleblowing> (дата обращения: 27.01.2025).

Sarbanes-Oxley Act (SOX). [Электронный ресурс]. — URL: https://www.whistleblowers.gov/statutes/sox_amended (дата обращения: 27.01.2025).

²¹ Корпоративные коммуникации тренды 2025, ключевые стратегии и инновации. [Электронный ресурс]. — URL: <https://svyazi-agency.ru/blog/korporativnye-kommunikacii-2024> (дата обращения: 27.01.2025).

интеграция этических каналов связи с общими системами корпоративного управления и ESG-принципами.²²

Анализ категорий нарушений, поступающих через корпоративные горячие линии, представленный в таблице 5, показывает доминирование вопросов, связанных с рабочим поведением и корпоративной культурой, что подчёркивает важность комплексного подхода к управлению рисками.

Таблица 5

**Структура сообщений по категориям
нарушений в корпоративных горячих линиях (2024 год)**

Категория нарушений	Доля сообщений (%)	Уровень подтверждения (%)	Медианный ущерб (тыс. USD)	Время расследования (дни)	Типичные последствия
Рабочее поведение	52,3	38	50	45	Дисциплинарные меры
Бухгалтерия и финансы	4,3	65	766	85	Увольнение, иски
Деловая этика	12,8	45	150	60	Обучение, корректировка
Растрата активов	18,7	55	120	70	Увольнение, возмещение
Коррупция	8,9	58	350	90	Правовые последствия
Кибербезопасность	3,0	42	280	30	Технические меры

Составлено автором на основе анализа материалов²³

Успешная реализация корпоративных горячих линий требует интеграции с общей системой управления рисками организации. Современные подходы предполагают создание единых центров обработки сообщений, объединяющих функции риск-менеджмента, внутреннего аудита, корпоративной безопасности и HR-служб. Ключевым элементом успеха является регулярное обучение персонала не только процедурам подачи сообщений, но и принципам этического поведения и распознавания признаков мошенничества²⁴

Развитие корпоративных мессенджеров и систем внутренней коммуникации в России создаёт новые возможности для интеграции функций сообщения о нарушениях в повседневные рабочие процессы. Рынок корпоративных коммуникаций в России оценивается в 81 миллиард рублей по итогам 2023 года с ожиданием удвоения к 2028 году²⁵, что создаёт благоприятные условия для внедрения продвинутых решений в области управления рисками.

Выводы

Проведённый сравнительный анализ нормативно-правовых подходов к регулированию корпоративных каналов сообщения о правонарушениях выявил существенные различия между юрисдикциями при наличии общих тенденций к усилению требований и расширению сферы

²² ESG-принципы — что это, зачем компаниям их соблюдать и как это делать. [Электронный ресурс]. — URL: <https://developers.sber.ru/help/business-development/esg-principles> (дата обращения: 27.01.2025).

²³ 2024 Whistleblowing & Incident Management Benchmark Report. [Электронный ресурс]. — URL: <https://www.navex.com/en-us/northstar/whistleblowing-incident-management-benchmark-report/> (дата обращения: 27.01.2025).

ACFE — Occupational Fraud 2024: A Report to the Nations. [Электронный ресурс]. — URL: <https://www.anchin.com/whitepapers/acfe-occupational-fraud-2024-a-report-to-the-nations/> (дата обращения: 27.01.2025).

²⁴ Внутрикorporативные расследования: 2024. [Электронный ресурс]. — URL: <https://tedo.ru/internal-corporate-investigations-2024> (дата обращения: 27.01.2025).

²⁵ Российский рынок корпоративных коммуникаций удвоится к 2028 г. [Электронный ресурс]. — URL: <https://www.comnews.ru/content/232508/2024-04-09/2024-w15/1008/rossiyskiy-rynok-korporativnykh-kommunikatsiy-udvoitsya-k-2028-g> (дата обращения: 27.01.2025).

применения. Американская модель, основанная на Законе Сарбейнса-Оксли, фокусируется на финансовой отчётности публичных компаний с жёсткими санкциями за несоблюдение, тогда как европейский подход, регламентированный Директивой ЕС 2019/1937, охватывает более широкий круг организаций и нарушений с акцентом на защите информаторов. Установлено, что международный стандарт ISO 37002:2021 предоставляет универсальную методологическую основу, применимую в различных регуляторных средах, что подтверждается его адаптацией в более чем 40 странах.

Исследование эволюции технологических решений продемонстрировало кардинальную трансформацию корпоративных горячих линий от простых телефонных систем к интегрированным цифровым платформам. Статистические данные NAVEX за 2024 год впервые зафиксировали превышение веб-отчётов (33,4 %) над телефонными сообщениями (29,4 %), что свидетельствует о предпочтениях пользователей в пользу более удобных и анонимных каналов. Выявлена прямая корреляция между технологической сложностью систем и их эффективностью: организации с мультиканальными платформами демонстрируют на 25–30 % более высокие показатели выявления нарушений при сокращении времени расследования на 40 %. Искусственный интеллект и машинное обучение становятся критически важными компонентами для автоматической классификации сообщений и выявления паттернов мошенничества.

Обоснованы принципы интегрированной модели создания эффективных систем внутрикорпоративного сообщения, основанной на шести ключевых компонентах: нормативно-правовое обеспечение, организационная структура, технологическая инфраструктура, процедуры обработки, система защиты информаторов и механизмы мониторинга эффективности. Модель предполагает адаптивность к различным регуляторным требованиям при сохранении единых стандартов качества и безопасности. Критически важным является обеспечение культуры доверия: организации с развитыми программами защиты от преследований демонстрируют в два раза более высокие показатели добровольных сообщений.

Общие выводы исследования подтверждают, что корпоративные горячие линии представляют собой наиболее эффективный инструмент выявления мошенничества, обеспечивающий детекцию 43 % всех случаев корпоративных злоупотреблений согласно глобальной статистике ACFE. Успешная реализация требует комплексного подхода, интегрирующего регуляторные требования, технологические инновации и культурные изменения в организации. Разработанная концептуальная модель обеспечивает методологическую основу для создания эффективных систем управления рисками мошенничества, способных адаптироваться к изменяющимся условиям глобальной экономики и эволюции регуляторных требований.

ЛИТЕРАТУРА

1. Басова, М.Е. Проблема применения комплаенса в противодействии корпоративному мошенничеству / М.Е. Басова // Право и экономика. — 2020. — № 3(385). — С. 44–48. — EDN QEYZET.
2. Губар, Н.Е. Риск экономического мошенничества как объект корпоративного управления / Н.Е. Губар // Защита информации. Инсайд. — 2011. — № 1(37). — С. 44–48. — EDN TMGICH.
3. Елаев, М.И. Опыт реализации антикоррупционного комплаенса в Банке ВТБ (ПАО) / М.И. Елаев // Гуманитарный научный журнал. — 2024. — № 2-2. — С. 143–147. — EDN RFGFAU.

4. Заброда, Д.Г. Методика антикоррупционного аудита: вопросы теории и практики / Д.Г. Заброда, А.В. Капранов — DOI 10.29039/2413-1733-2021-7-3(2)-187-199. // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. — 2021. — Т. 7(73), № 3-2. — С. 187–199 — EDN CFPADL.
5. Кабанова, Н.А. Система противодействия основным схемам корпоративного мошенничества в компаниях молочной отрасли / Н.А. Кабанова, Д.Д. Накостик // Транспортное дело России. — 2020. — № 2. — С. 48–50. — EDN HJSAGE.
6. Садыржанов, Б.Э. Противодействие корпоративному мошенничеству в системе экономической безопасности в России и за рубежом / Б.Э. Садыржанов // Экономика. Бизнес. Банки. — 2020. — № 3(41). — С. 125–132. — EDN DGYKKU.
7. Семенов, Н.С. Совершенствование системы противодействия корпоративному мошенничеству в сфере закупок ПАО "НК "Роснефть" / Н.С. Семенов // Самоуправление. — 2020. — № 4(121). — С. 454–457. — EDN YMMROU.
8. Снимщикова, И.В. Антикоррупционная политика как фактор противодействия корпоративному мошенничеству в нефтяных компаниях / И.В. Снимщикова, А.Б. Мельников, Ю.А. Чугаева — DOI 10.37493/2307-907X.2020.1.18. // Вестник Северо-Кавказского федерального университета. — 2020. — № 1(76). — С. 151–157 — EDN LDWSQG.
9. Сотов, А.И. Организация "горячей линии" компании в целях противодействия коррупции: европейский опыт комплаенса / А.И. Сотов — DOI 10.18572/2072-442X-2022-2-27-30. // Эксперт-криминалист. — 2022. — № 2. — С. 27–30. — EDN DHDPOM.
10. Сулейманов, С.К. Механизмы противодействия корпоративному мошенничеству / С.К. Сулейманов — DOI 10.24411/2076-1503-2020-10651. // Образование и право. — 2020. — № 6. — С. 335–339 — EDN QGCPGQ.
11. Чумак, Г.В. Применение метода ручной оценки контрагентов при противодействии корпоративному мошенничеству / Г.В. Чумак, А.Е. Суглобов, Е.А. Телкова — DOI 10.29039/2409-6024-2022-10-1-71-75. // Russian Journal of Management. — 2022. — Т. 10, № 1. — С. 71–75 — EDN XQGZNE.
12. Южакова, Н.А. Механизмы выявления и регулирования оппортунистического поведения персонала в компании / Н.А. Южакова — DOI 10.35854/1998-1627-2024-4-511-520. // Экономика и управление. — 2024. — Т. 30, № 4. — С. 511–520 — EDN MIJFXK.

Biryukov Vyacheslav Vitalievich

Financial University under the Government of the Russian Federation, Moscow, Russia

E-mail: birslava2004@mail.ru

ORCID: <https://orcid.org/0009-0000-2010-1923>

Organizational and methodological foundations for creating corporate hotlines to combat fraud based on international experience

Abstract. The modern globalized economic environment is characterized by increasing risks of corporate fraud, requiring organizations to develop effective counteraction mechanisms, among which corporate hotlines are of particular importance as a tool for early detection and prevention of financial violations. This study presents a comprehensive analysis of international experience in the creation and operation of corporate fraud reporting systems, including a study of the regulatory framework of leading jurisdictions, methodological approaches to organizing internal corporate communication channels and technological solutions to ensure the effectiveness of offense detection. The study covers the analysis of the evolution of conceptual approaches from classic internal control models to modern integrated risk management systems that take into account the specifics of digital transformation and changed regulatory requirements. Particular attention is paid to a comparative analysis of the American model based on the requirements of the Sarbanes-Oxley Act, the European approach regulated by the EU Whistleblower Protection Directive, and emerging practices in the jurisdictions of the Asia-Pacific region. The conducted analysis of statistical data from the Association of Certified Fraud Examiners for 2024 shows that reports through internal channels remain the most effective way to detect corporate fraud, accounting for 43 % of all detection cases, with median losses for organizations of USD 1,662 million per case. The results of the study indicate the need to move from traditional telephone hotlines to multi-channel digital platforms integrating web forms, mobile applications and artificial intelligence tools to analyze incoming reports. The developed conceptual model of organizational and methodological foundations includes six key components: regulatory framework, organizational structure, technological infrastructure, message processing procedures, whistleblower protection system and performance monitoring mechanisms.

Keywords: corporate hotlines; fraud prevention; internal control; risk management; international standards; digital transformation; corporate governance; whistleblower protection; financial violations