А. Л. Кудряшов

# Экономическая разведка и противодействие финансовым угрозам в российских компаниях

*Монография*

А. Л. Кудряшов

# Экономическая разведка и противодействие финансовым угрозам в российских компаниях. Монография

**Кудряшов А. Л.**

Экономическая разведка и противодействие финансовым угрозам в российских компаниях. Монография / А. Л. Кудряшов —

Монография посвящена вопросам экономической разведки и противодействия финансовым угрозам в российских компаниях. Исследованы теоретические аспекты защиты корпоративных интересов, источники и признаки финансовых рисков, методы выявления угроз, порядок аналитической оценки и организационные решения по укреплению устойчивости бизнеса. Издание адресовано исследователям, преподавателям, аспирантам, магистрантам и практикам.

# Содержание

# Экономическая разведка и противодействие финансовым угрозам в российских компаниях Монография

## А. Л. Кудряшов



ISBN 978-5-0069-9005-0
Создано в интеллектуальной издательской системе Ridero

# ВВЕДЕНИЕ

Настоящая монография посвящена вопросам организации экономической разведки и противодействия финансовым угрозам в деятельности российских компаний. Выбор предмета обусловлен изменениями хозяйственной среды, произошедшими в последние годы: расширением санкционных ограничений, перестройкой платежных маршрутов, ростом цифровых угроз и усложнением контрагентских связей. Эти обстоятельства потребовали пересмотра подходов к защите финансовых интересов организаций и обусловили необходимость разработки новых аналитических инструментов.

Экономическая безопасность организации рассматривается в монографии как способность компании сохранять непрерывность деятельности, защищать активы и своевременно исполнять обязательства даже при неблагоприятных воздействиях. Данное понимание восходит к работам В. К. Сенчагова, А. Е. Городецкого, И. В. Караваевой и других отечественных исследователей, заложивших теоретическую основу дисциплины. Международный контекст определяется документами COSO, ISO, FATF, OECD, IFC, содержащими апробированные методики управления рисками и внутреннего контроля. Исследования A. Cavallo, L. Madureira, S. Ainslie, D. Cheng, J. Sorensen вносят вклад в понимание корпоративной разведки, анализа угроз и обнаружения мошенничества.

Вместе с тем существующие модели оценки финансовых угроз не учитывают ряд обстоятельств, значимых для российских компаний. Стандартные матрицы рисков оперируют двумя параметрами (вероятностью и последствиями) и не принимают во внимание ни качество обнаружения, ни уязвимость процедуры, ни необратимость последствий. Метод FMEA, применяемый в инженерной практике, ближе по конструкции, однако не содержит показателя необратимости. Ни одна из известных автору корпоративных моделей не учитывает каскадного взаимодействия между одновременно действующими угрозами и не измеряет продолжительность скрытого периода угрозы.

Указанные пробелы определили направленность исследования. В монографии разработаны шесть взаимосвязанных инструментов оценки: индекс финансовой угрозы с учетом необратимости (ИФУН), коэффициент снижения угрозы (Ксн), коэффициент межугрозового усиления (КМУ), скорректированный индекс (ИФУН_скорр), коэффициент латентности (Кл) и коэффициент уровня экономической безопасности (КУЭБ). Каждый из инструментов подробно обоснован, снабжен правилами присвоения значений и проиллюстрирован на анонимизированном расчетном примере.

Книга адресована исследователям и практикам в области экономической безопасности, финансового анализа и корпоративного управления. Она может быть полезна руководителям компаний, специалистам аналитических подразделений, внутренним аудиторам, преподавателям и студентам, изучающим экономическую безопасность.

Монография состоит из трех глав. Первая глава раскрывает теоретико-методологические основы экономической разведки и финансовой безопасности: уточняет понятийный аппарат, систематизирует финансовые угрозы и анализирует существующие методологические подходы к оценке. Вторая глава посвящена практике организации экономической разведки в российских компаниях, механизмам обнаружения угроз и авторской модели оценки (ИФУН, КМУ, Кл). Третья глава содержит методику обобщенной оценки состояния компании (КУЭБ), рекомендации по внедрению и анализ организационных условий результативности.

# ГЛАВА 1. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ЭКОНОМИЧЕСКОЙ РАЗВЕДКИ И ФИНАНСОВОЙ БЕЗОПАСНОСТИ

## 1.1. Эволюция концепции экономической безопасности и экономической разведки

Категория экономической безопасности вошла в отечественный научный оборот в начале 1990-х годов, когда распад централизованной хозяйственной системы поставил перед исследователями и органами государственного управления вопрос о допустимых границах воздействия на экономику страны. Прежние модели директивного планирования утрачивали силу, рыночные институты еще не сложились, а масштаб угроз – от спада промышленного производства и деиндустриализации до вывоза капитала и нарастания внешнего долга – требовал нового понятийного аппарата. Работы Л. И. Абалкина, В. К. Сенчагова, Е. А. Олейникова, выполненные в этот период, заложили основу, которая к середине 2000-х годов приобрела относительно устоявшийся характер [7]. Данные исследования исходили из того, что экономическая безопасность представляет собой состояние национальной экономики, при котором обеспечивается защита жизненно значимых интересов государства, общества и личности от внутренних и внешних угроз.

Содержание первых определений носило преимущественно макроэкономический характер. Индикаторный перечень включал темпы роста валового внутреннего продукта, уровень инфляции, состояние платежного баланса, долю импорта продовольствия и критического оборудования, объем государственного долга, степень долларизации внутреннего оборота. Подобная направленность соответствовала актуальным вызовам того времени. К середине 1990-х годов Россия утратила значительную часть промышленного потенциала, объем вывоза капитала многократно превышал прямые иностранные инвестиции, а бюджетная система находилась в состоянии хронического дефицита. Безопасность воспринималась прежде всего как предотвращение катастрофического ухудшения макроэкономических показателей, а корпоративный уровень рассматривался преимущественно через призму занятости, налоговых поступлений и социальной устойчивости.

По мере стабилизации экономической ситуации в стране акцент научных исследований начал смещаться. К середине 2000-х годов стало очевидным, что макроэкономическая устойчивость реализуется через финансовое состояние конкретных организаций, качество их управленческих решений и характер хозяйственных связей. Приватизация, формирование фондового рынка, рост числа посредников и подрядчиков, появление сложных финансовых инструментов и расширение международных связей поставили перед компаниями вопрос о сохранности активов, устойчивости расчетов и надежности деловых партнеров. Появились работы, рассматривающие экономическую безопасность предприятия как самостоятельный предмет исследования. Жариков (2021) систематизировал учебный материал по экономической безопасности государства, однако и на уровне учебного пособия подчеркнул связь макро- и микроуровней [12]. Докучкина (2023) систематизировала теоретические основы концепции экономической безопасности предприятия применительно к условиям цифровой трансформации, показав, что появление новых технологий одновременно расширяет инструментарий защиты и порождает ранее неизвестные источники угроз [13].

Период 2010-х годов ознаменовался усилением внимания к институциональным аспектам безопасности. Исследователи обратились к вопросам качества корпоративного управления, прозрачности финансовой отчетности, эффективности внутреннего контроля и роли аудита в предупреждении финансовых потерь. Буряков и соавторы (2011) в коллективной монографии рассмотрели экономическую безопасность и финансовую устойчивость предприятий как взаимосвязанные характеристики, указав на необходимость соединения финансового анализа с оценкой организационных уязвимостей [5]. Этот взгляд оказался важен для последующего развития концепции, поскольку позволил расширить предмет исследования за пределы традиционного финансового анализа.

Нормативное закрепление многоуровневого понимания экономической безопасности произошло в 2017 году с принятием Стратегии экономической безопасности Российской Федерации на период до 2030 года. Указ Президента Российской Федерации от 13.05.2017 No 208 определил экономическую безопасность как состояние защищенности национальной экономики от внешних и внутренних угроз, при котором обеспечиваются экономический суверенитет страны, единство ее экономического пространства, условия для реализации стратегических приоритетов Российской Федерации. Документ выделил основные вызовы и угрозы, установил цели и направления государственной политики, определил порядок оценки состояния экономической безопасности на основе системы показателей. Среди вызовов названы стремление отдельных стран использовать экономические методы для достижения политических целей, усиление структурных дисбалансов в мировой экономике, повышение конфликтного потенциала в зонах экономических интересов, а также рост масштабов теневой экономики и криминализация хозяйственных отношений [1].

Стратегия национальной безопасности Российской Федерации (Указ Президента от 02.07.2021 No 400) связала экономическую составляющую с задачами защиты информации, критической инфраструктуры и финансовой стабильности. Документ определил национальные интересы, стратегические приоритеты и механизмы обеспечения безопасности, включив корпоративный уровень в общую систему защиты. Для настоящего исследования существенно, что оба документа рассматривают безопасность как многоуровневую систему, в которой государственный и корпоративный уровни связаны, но не тождественны: защита национальных интересов реализуется, в частности, через устойчивость хозяйствующих субъектов, а состояние компаний, в свою очередь, определяется как общей экономической средой, так и качеством собственного управления [2].

Городецкий и Караваева (2023) в коллективной монографии Института экономики Российской академии наук обосновали необходимость рассматривать экономическую безопасность как многоуровневую систему, в которой корпоративный уровень выполняет роль фундамента: от финансового состояния организаций зависит устойчивость отраслей, регионов и экономики в целом. Авторы подчеркнули, что теоретическое обоснование экономической безопасности неотделимо от вопросов государственного регулирования и что методы оценки должны учитывать специфику институциональной среды [16].

Для настоящего исследования принципиальное значение имеет переход от макроэкономического понимания к корпоративному. На уровне организации безопасность приобретает конкретное управленческое содержание: речь идет о способности компании сохранять непрерывность деятельности, защищать активы, своевременно исполнять обязательства и воспроизводить капитал даже при неблагоприятных воздействиях. Данное понимание опирается на работы отечественных исследователей, рассматривающих экономическую безопасность организации через сохранность ее имущественных интересов и устойчивость финансовых процессов.

Финансовая безопасность занимает внутри корпоративной системы экономической безопасности первостепенное положение. Через денежные потоки, обязательства, ликвидность

и качество финансовой информации проявляется большинство корпоративных уязвимостей. Брагина и Круц (2023) обоснованно рассматривают финансовую безопасность как форму экономической безопасности, соединяющую устойчивость финансового состояния и защищенность от потерь, вызванных ошибками, злоупотреблениями и внешними воздействиями [15]. Левкина, Лялина, Локша и Савостина (2022) предложили многоуровневый подход к финансовым аспектам обеспечения экономической безопасности, охватывающий макро-, мезо- и микроуровни. Данный подход позволяет рассматривать финансовую безопасность конкретной организации в контексте отраслевых и макроэкономических условий, что особенно существенно для компаний, зависящих от состояния внешних рынков или государственного финансирования [4].

Сапожникова и Рейхерт (2021) предприняли попытку систематизировать теоретические и практические подходы к экономической безопасности, указав на необходимость увязывания теоретических построений с конкретными инструментами корпоративного управления. Авторы подчеркнули, что сама по себе констатация наличия угроз не образует научного результата; значение имеет разработка методики, позволяющей количественно или хотя бы ранжировочно оценить степень опасности и выбрать адекватное решение [3].

Понятийная строгость требует разграничения нескольких категорий, которые в литературе и профессиональной среде нередко употребляются как синонимы. Риск выражает вероятность неблагоприятного результата и его возможный масштаб. Данное понятие восходит к классическим работам Ф. Найта, разграничившего риск (измеримую неопределенность) и неопределенность (неизмеримую). Для целей корпоративного анализа существенно, что риск может быть описан через статистическую вероятность или экспертную оценку, но сам по себе еще не содержит указания на конкретного носителя или механизм причинения ущерба.

Угроза предполагает наличие источника воздействия и описываемого способа реализации. Источником может выступать недобросовестный контрагент, должностное лицо со злоумышленными намерениями, системное ограничение внешней среды (санкции, валютные ограничения), сбой информационной системы или иное обстоятельство, обладающее направленностью и способностью причинить ущерб. В отличие от риска, угроза всегда конкретна: она указывает не только на вероятность, но и на то, кто (или что) выступает носителем опасности и каким образом воздействие может осуществиться.

Уязвимость показывает, в каком месте система управления оказывается недостаточно защищенной и где угроза получает возможность реализоваться. Незащищенный платежный канал, отсутствие двойного подтверждения операций, формальная проверка контрагентов, совмещение несовместимых функций одним должностным лицом – все это примеры организационных уязвимостей. Их наличие само по себе не означает наступления ущерба (для этого необходим активный источник угрозы), однако повышает вероятность реализации неблагоприятного события.

Ущерб фиксирует уже наступившее последствие: прямые финансовые потери, утрату имущества, штрафные санкции, удорожание обслуживания обязательств, необходимость привлечения дополнительного финансирования или ухудшение деловой репутации. Существенно, что последствия финансовой угрозы не исчерпываются непосредственным денежным ущербом: они могут включать утрату деловых связей, осложнение отношений с регуляторами, снижение кредитоспособности и долгосрочное ухудшение конкурентных позиций.

Практическая ценность этого разграничения проявляется при принятии управленческих решений. Когда руководитель компании получает сигнал о возможной опасности, характер принимаемого решения существенно зависит от того, идет ли речь о статистической вероятности некоторого события (риск), о конкретном источнике воздействия (угроза), о слабости защитной процедуры (уязвимость) или о состоявшихся потерях (ущерб). Смешение этих понятий ведет к тому, что защитные меры оказываются несоразмерными: избыточное реагирова-

ние на умеренные риски истощает ресурсы контроля, а недостаточное внимание к конкретным угрозам оставляет компанию незащищенной. Наумова и Тюгин (2018) предложили методику мониторинга финансовой безопасности хозяйствующего субъекта на основе оценки финансовых угрожающих рисков, подчеркнув необходимость разделения текущих и потенциальных опасностей [6]. Naumova и Svetkina (2019) развили данный подход в англоязычной публикации, показав, что индикаторное наблюдение дает положительные результаты при условии регулярности и методической последовательности [11].

Финансовая безопасность организации включает две взаимосвязанные характеристики: устойчивость и защищенность. Устойчивость описывает способность компании поддерживать платежеспособность, приемлемую структуру источников финансирования и воспроизводство капитала на протяжении рассматриваемого периода. Она проявляется в показателях ликвидности, долговой нагрузки, оборачиваемости и доходности. Защищенность показывает готовность предупреждать и пресекать потери, вызванные злоупотреблениями, договорными нарушениями, ошибками учета, внешними ограничениями и цифровыми посягательствами. Она проявляется в качестве внутреннего контроля, надежности процедур согласования, полноте проверки контрагентов и защищенности информационной среды. Эти свойства не тождественны, однако в хозяйственной практике проявляются совместно: ослабление своевременности платежей подрывает устойчивость, а ухудшение финансового положения облегчает реализацию угроз.

Корпоративный характер экономической безопасности имеет системное значение. Именно на уровне организации происходят сбои расчетов, ухудшаются условия расчетов с контрагентами, растет стоимость заемного финансирования, обнаруживается уязвимость цепочек поставок и проявляются последствия внешних ограничений. От состояния компаний зависит устойчивость отраслей и регионов; совокупность корпоративных финансовых состояний образует основу макроэкономической устойчивости. Данный взгляд приобретает особую актуальность в условиях санкционных и геоэкономических ограничений, когда внешнее воздействие реализуется через вполне конкретные финансовые и договорные механизмы: блокировку корреспондентских счетов, ограничение доступа к международным платежным системам, запрет на отдельные виды сделок, заморозку активов.

Близкий, Свистунов и Гулуа (2022) рассмотрели вопросы экономической безопасности через призму учетно-аналитической системы организации и показали, что формирование адекватной информационной базы для принятия управленческих решений составляет необходимое условие защиты от финансовых потерь. Авторы обратили внимание на типичные недостатки учетных систем: неполноту отражения хозяйственных операций, запоздалость предоставления информации, несогласованность данных управленческого и бухгалтерского учета. Каждый из этих недостатков создает информационную уязвимость, которая может быть использована для совершения финансовых злоупотреблений [17].

Экономическая разведка как самостоятельная корпоративная функция сформировалась по мере усложнения хозяйственной среды. Расширение сетей контрагентов, нарастание информационной асимметрии, появление сложных финансовых инструментов и рост числа посредников породили потребность в целенаправленной проверке деловой репутации, структуры владения, своевременности расчетов и фактической устойчивости партнеров. Решить подобные задачи средствами бухгалтерского учета или стандартного финансового анализа невозможно. Они требуют сопоставления внутренних и внешних данных, правовой информации, отраслевого контекста и сведений из открытых источников. Именно это обстоятельство обусловило выделение экономической разведки в самостоятельное направление корпоративной деятельности [4, 7].

В настоящей работе экономическая разведка определяется как упорядоченная аналитическая деятельность по законному сбору, проверке, сопоставлению и интерпретации сведений,

имеющих значение для предупреждения финансового ущерба. Ее результатом служат аналитические выводы, отделяющие факт от предположения и гипотезу от подтвержденного обстоятельства. Данное определение сознательно отграничивает экономическую разведку от негласных и противоправных методов получения информации, от деятельности государственных спецслужб и от промышленного шпионажа. Предмет экономической разведки в корпоративном понимании – информация, необходимая для предупреждения финансового ущерба, получаемая законным путем из открытых и санкционированных источников.

Стратегическое значение экономической разведки определяется тем, что наиболее значимые корпоративные решения принимаются при неполноте информации. Выбор контрагентов, моделей финансирования, инвестиционных направлений и способов защиты активов всегда сопряжен с неопределенностью. Экономическая разведка снижает эту неопределенность, позволяя проверить исходные условия решения, оценить финансовую состоятельность партнера, выявить скрытые уязвимости и установить обстоятельства, при которых возможна реализация угрозы. Ее результаты должны быть представлены в форме, пригодной для управленческого решения: с указанием установленных фактов, степени их подтвержденности, оценки вероятности и масштаба возможных последствий, а также конкретных предложений по действию.

Для методической определенности необходимо разграничить экономическую разведку с тремя смежными корпоративными функциями: внутренним контролем, аудитом и деятельностью по соблюдению обязательных требований. Это разграничение не означает изоляции: перечисленные функции связаны между собой и обмениваются результатами. Однако различие их предмета, временного горизонта и характера доказательств принципиально для понимания места каждой из них в системе корпоративного управления.

Внутренний контроль, как его определяет COSO Internal Control – Integrated Framework (2013), обеспечивает разумную уверенность в достижении целей операционной эффективности, достоверности отчетности и соблюдения применимого законодательства. Он включает пять компонентов: контрольную среду, оценку рисков, контрольные действия, информирование и коммуникацию, мониторинг. Внутренний контроль сосредоточен на текущих операциях и на соблюдении утвержденного порядка [33]. Воюцкая, Коське и Мишучкова (2022) исследовали потенциал внутреннего контроля в выявлении рисков искажения бухгалтерской отчетности и показали, что его результативность определяется полнотой охвата хозяйственных операций и квалификацией исполнителей [14]. Экономическая разведка опирается на данные внутреннего контроля, однако работает с иным предметом: она анализирует потенциальные угрозы, которые могут реализоваться при изменении поведения контрагента, структуры сделки, финансового состояния партнера или внутриорганизационных условий. Различие определяется прежде всего временным горизонтом: контроль фиксирует текущее состояние, разведка прогнозирует будущее ухудшение.

Аудит, регулируемый Федеральным законом от 30.12.2008 No 307-ФЗ об аудиторской деятельности и международными стандартами аудита, строится как регламентированная проверка отчетности или отдельных участков учета на основе установленного набора процедур [22]. Пересмотренный стандарт ISA 240 (2025) прямо указывает на обязанность аудитора рассматривать риски мошенничества при проверке финансовой отчетности и применять профессиональный скептицизм при оценке допущений руководства [21]. Экономическая разведка использует результаты аудита, но собирает и сопоставляет разнородные сведения: о структуре владения контрагентов, судебных спорах, финансовом положении деловых партнеров, ограничительных мерах и иных обстоятельствах, влияющих на вероятность ущерба. Ее вывод не равен аудиторскому заключению и не заменяет его; это управленческое суждение, основанное на совокупности доказательств различной природы.

Деятельность по соблюдению обязательных требований (комплаенс) оценивает соответствие действий компании законодательству, нормативным ограничениям и внутренним политикам. Федеральный закон от 07.08.2001 No 115-ФЗ о противодействии легализации доходов, полученных преступным путем, обязывает организации, осуществляющие операции с денежными средствами, проводить идентификацию клиентов и сообщать о подозрительных операциях [8]. Рекомендации FATF (2012, с изменениями на 2025 год) предусматривают применение усиленной проверки при повышенном уровне риска [34]. Руководство OECD по внутреннему контролю, этике и соответствию (2010) устанавливает ожидания в отношении создания каналов сообщения о нарушениях и защиты лиц, сообщающих о злоупотреблениях [53]. Экономическая разведка учитывает требования комплаенса, однако рассматривает более широкий круг обстоятельств. Снижение платежеспособности контрагента, концентрация зависимости в одном звене цепочки поставок, рост использования уязвимого платежного канала или появление у приоритетного работника необъяснимых внешних доходов – все это может оставаться в пределах правового поля, однако представлять реальную угрозу для компании.


Рисунок 1 – Структура системы экономической безопасности компании

*Источник: составлено автором.*

На рисунке 1 представлена структура системы экономической безопасности компании. Финансовая безопасность выступает основной составляющей, поскольку именно через денежные потоки и обязательства проявляется большинство корпоративных уязвимостей. Устойчивость денежных потоков, защищенность активов, платежный порядок, достоверность информации и кадровая безопасность образуют пять взаимосвязанных блоков. Экономическая разведка обеспечивает аналитическую поддержку каждого из них, обрабатывая сведения из внутренних и внешних источников.


Рисунок 2 – Место экономической разведки в системе корпоративного управления

*Источник: составлено автором.*

Рисунок 2 демонстрирует, что экономическая разведка выполняет связующую функцию между несколькими корпоративными подразделениями. Она получает данные от финансовой службы, юридического отдела, службы безопасности, подразделения информационной безопасности и подразделения внутреннего контроля, обрабатывает их и представляет выводы руководству компании. При отсутствии специализированной аналитической функции сведения о потенциальных угрозах рассеиваются между подразделениями, а руководитель принимает решение на основании неполной картины.

Зарубежный опыт организации корпоративной разведки представляет интерес, хотя прямой перенос его в российскую среду затруднен различиями правовых систем, деловой культуры и институциональной структуры. В англоязычной литературе используются термины competitive intelligence (конкурентная разведка), business intelligence (деловая аналитика) и corporate intelligence (корпоративная разведка). Содержание этих понятий частично пересекается, но не совпадает. Competitive intelligence ориентирована преимущественно на сбор и анализ информации о конкурентах и рыночной среде для поддержки стратегических решений. Business intelligence в современном понимании означает использование аналитических инструментов для обработки корпоративных данных и поддержки принятия решений. Corporate intelligence охватывает более широкий круг задач, включая проверку деловых партнеров, оценку рисков и защиту корпоративных интересов.

Cavallo, Sanasi, Ghezzi и Rangone (2021) исследовали связь конкурентной разведки со стратегическим планированием, проведя систематический обзор литературы, и установили, что ее результативность определяется не столько объемом собираемых данных, сколько качеством интеграции аналитических выводов в процесс принятия стратегических решений. Авторы подчеркнули, что разрыв между сбором информации и ее использованием в управлении является одной из наиболее распространенных причин неэффективности разведыва-

тельных функций [35]. Madureira, Popovic и Castelli (2021) предложили модульное определение конкурентной разведки, выделив аналитическую, информационную и организационную составляющие. Подобная модульная структура позволяет адаптировать разведывательную функцию к масштабу и специфике организации [36]. Dvojmoc (2019) рассмотрел корпоративную разведку как обязательный элемент глобального бизнеса, обусловленный усложнением деловых связей и ростом информационных угроз [37]. Sidak, Zakharov и Zaplatynskyi (2018) обосновали значение конкурентной разведки для экономической безопасности предприятий, обратив внимание на роль информационного обеспечения в условиях нарастающей конкуренции и цифровизации [38].

Цифровизация привнесла новый аналитический инструментарий и одновременно новые угрозы. Ainslie, Thompson, Maynard и Ahmad (2023) показали, что анализ киберугроз (cyber-threat intelligence) все теснее связывается с принятием управленческих решений в области безопасности, поскольку цифровые инциденты влекут прямые финансовые последствия. Авторы провели систематический обзор литературы и сформулировали исследовательскую повестку, указав на необходимость интеграции анализа киберугроз в общую систему корпоративного управления рисками [39]. Scuro (2026) систематизировал методы разведки по открытым источникам (OSINT) применительно к исследовательской практике, показав, что основой результативной работы служат методическая последовательность и верификация данных. Для экономической разведки в компании эти методы применимы при проверке контрагентов, анализе структуры владения и оценке деловой репутации [45].

Институциональная среда российского бизнеса оказывает существенное влияние на организацию экономической разведки. Высокая степень концентрации собственности, характерная для крупных и средних отечественных компаний, порождает специфические конфликты интересов. Мажоритарный собственник нередко обладает прямым доступом к чувствительной информации и влиянием на кадровые решения; в подобных условиях экономическая разведка может превращаться в инструмент контроля собственника над наемным менеджментом. В компаниях с распыленной собственностью аналитическая функция чаще ориентирована на защиту интересов совета директоров и миноритарных акционеров. Принципы G20/OECD Principles of Corporate Governance (2023) устанавливают общие ожидания в отношении прозрачности, подотчетности и защиты прав участников корпоративных отношений [50].

Правовая основа экономической разведки в российской компании складывается из нескольких групп нормативных актов. Федеральный закон от 06.12.2011 No 402-ФЗ о бухгалтерском учете устанавливает требования к достоверности учета и отчетности. Федеральный закон от 29.07.2004 No 98-ФЗ о коммерческой тайне определяет условия отнесения сведений к коммерческой тайне, порядок их защиты и ответственность за разглашение [30]. Федеральный закон от 27.07.2006 No 152-ФЗ о персональных данных регламентирует условия обработки персональных данных работников и контрагентов [31]. Федеральный закон от 26.07.2017 No 187-ФЗ о безопасности критической информационной инфраструктуры устанавливает требования к защите информационных систем, нарушение функционирования которых может повлечь существенные последствия [18]. Отсутствие специального закона об экономической разведке или корпоративных расследованиях означает, что каждая операция по сбору и обработке информации должна оцениваться с точки зрения соответствия перечисленным нормам.

Хусаинова, Савельева, Подыганова и Дятлова (2024) рассмотрели механизмы и инструменты разработки и внедрения эффективной системы экономической безопасности предприятия, отметив, что организационные барьеры нередко оказываются более значимым препятствием, чем отсутствие технических решений. Авторы указали на необходимость целенаправленной работы с организационной культурой и на важность поддержки со стороны выс-

шего руководства для обеспечения результативности системы безопасности [16 по списку оригинала].

Подводя итог подглавы, зафиксируем несколько положений, имеющих значение для дальнейшего исследования. Экономическая безопасность компании представляет собой многоуровневую систему, связывающую финансовую устойчивость, защищенность от внешних и внутренних воздействий и качество информационного обеспечения управленческих решений. Финансовая безопасность составляет ее ядро, поскольку именно через финансовые процессы реализуется большинство корпоративных угроз. Экономическая разведка выполняет в этой системе аналитическую функцию, содержательно отличную от внутреннего контроля, аудита и комплаенса по предмету, временному горизонту и характеру доказательств. Ее место в корпоративном управлении определяется потребностью руководства в своевременной, проверенной и управленчески значимой информации о формирующихся угрозах. Дальнейшее исследование требует перехода к анализу конкретных финансовых угроз и методологических подходов к их оценке.

## 1.2. Финансовые угрозы в системе экономической безопасности российских компаний

Содержание понятия финансовой угрозы определяется возможностью наступления обстоятельств, при которых компания утрачивает активы, несет непредвиденные расходы, лишается части доходов или оказывается в положении, затрудняющем исполнение принятых обязательств. Угроза отличается от общего понятия финансового риска наличием трех элементов: источника воздействия, описываемого механизма реализации и прогнозируемых последствий для конкретного участка деятельности. Именно совокупность этих элементов позволяет перейти от абстрактного указания на возможные неблагоприятные последствия к конкретному описанию того, каким путем и при каких обстоятельствах компания может понести ущерб [6, 9].

Кондрашова и Фаустов (2025) рассмотрели финансовую составляющую экономической безопасности в контексте обновленной системы угроз и указали на расширение их перечня и усложнение механизмов реализации. Авторы обратили внимание на то, что традиционное деление угроз на внутренние и внешние не исчерпывает всего многообразия современных ситуаций: значительная часть угроз имеет смешанную природу, поскольку внешний источник воздействия проникает в организацию через внутреннюю уязвимость [9]. Данное наблюдение имеет прямое значение для организации экономической разведки: аналитик не может ограничиваться одним направлением анализа (только внутренним или только внешним), а должен рассматривать угрозу в совокупности ее составных элементов.

Финансовые угрозы в деятельности российских организаций имеют неоднородную природу. Часть из них обусловлена внутренними обстоятельствами: ошибками при согласовании платежей, злоупотреблениями при заключении договоров, искажением учетных данных, конфликтом интересов должностных лиц, совмещением несовместимых функций в одном лице. Другая часть порождена внешними факторами: неплатежеспособностью контрагента, санкционными ограничениями, мошенническими действиями третьих лиц, изменениями нормативных требований, нарушениями информационной безопасности. Существует и промежуточная категория: угрозы, в которых внешнее воздействие реализуется вследствие внутренней уязвимости.

Предлагаемая в настоящей работе классификация финансовых угроз опирается на два критерия: источник опасности и механизм реализации. По источнику выделяются четыре группы. Первая – внутренние угрозы, порождаемые действиями или бездействием работников и должностных лиц организации. К ним относятся: злоупотребление полномочиями при распоряжении денежными средствами и имуществом, фальсификация первичных документов, присвоение активов, нецелевое использование корпоративных ресурсов, сокрытие существенной информации от руководства, дробление платежей для обхода установленных лимитов согласования, заключение договоров с аффилированными структурами при сокрытии заинтересованности, умышленное искажение управленческой или бухгалтерской отчетности.

Вторая группа – внешние угрозы, связанные с действиями контрагентов, конкурентов, регуляторов или иных участников хозяйственной среды. К ним относятся: ненадлежащее исполнение договорных обязательств, предоставление ложных сведений о финансовом состоянии или структуре владения, санкционные ограничения, изменение условий доступа к платежной инфраструктуре, односторонние действия банков по ограничению операций, изменение регуляторных требований, затрагивающее финансовую деятельность организации.

Третья группа – цифровые угрозы: несанкционированный доступ к информационным системам, подмена данных в системах учета и расчетов, компрометация платежных каналов, использование методов социальной инженерии для получения доступа к финансовым дан-

ным, внедрение вредоносного программного обеспечения в корпоративную информационную среду.

Четвертая группа – угрозы, связанные с недобросовестным поведением участников хозяйственного оборота: корпоративное мошенничество (fraud), фиктивные операции, создание подставных организаций для вывода денежных средств, манипулирование закупочными ценами, организация фиктивных тендеров.

По механизму реализации различаются четыре способа воздействия. Прямое воздействие на активы и обязательства: хищение денежных средств, незаконное списание имущества, перенаправление платежей на подставные счета, создание необоснованных обязательств. Искажение информации: фальсификация отчетности, подмена платежных реквизитов, сокрытие данных о финансовом состоянии контрагента, уничтожение или подмена первичных документов. Нарушение порядка принятия решений: обход установленных процедур согласования, несоблюдение утвержденных лимитов, принятие решений за пределами предоставленных полномочий. Воспрепятствование контролю: ограничение доступа аудиторов или контрольных подразделений к данным, уничтожение документов, оказание давления на лиц, выявивших нарушения.


Рисунок 3 – Классификация финансовых угроз

*Источник: составлено автором.*

Рисунок 3 систематизирует основные группы финансовых угроз с указанием конкретных видов в каждой группе. Классификация позволяет определить, какие подразделения компании отвечают за выявление конкретной группы угроз, какие источники данных необходимы для их обнаружения и какие аналитические методы применимы в каждом случае. Внутренние угрозы выявляются преимущественно подразделениями внутреннего контроля и аудита; внешние –

службой экономической разведки и комплаенса; цифровые – подразделением информационной безопасности; мошенничество – совместными усилиями нескольких подразделений.

Внутренние угрозы заслуживают наиболее пристального рассмотрения, поскольку именно они с наибольшим трудом поддаются обнаружению стандартными контрольными процедурами. Лицо, совершающее злоупотребление, как правило, обладает легитимным доступом к соответствующим операциям, знает порядок контроля и способно адаптировать свои действия к действующим ограничениям. ISA 240 (Revised, 2025) прямо указывает на преднамеренный характер мошенничества и его направленность на сокрытие [21]. Руководство COSO и ACFE по управлению рисками мошенничества (Fraud Risk Management Guide, 2023) обобщает статистику корпоративных потерь и формулирует рекомендации по профилактике, выявлению и расследованию [52]. По данным ACFE, медианный срок до обнаружения корпоративного мошенничества составляет от двенадцати до восемнадцати месяцев, а медианные потери по одному эпизоду превышают сто тысяч долларов.

Концептуальной основой анализа корпоративного мошенничества служит модель треугольника мошенничества, предложенная Д. Кресси. Мошенничество возникает при совпадении трех обстоятельств: давления (финансовые затруднения, карьерные ожидания, зависимость), возможности (уязвимость процедуры, отсутствие надлежащего контроля, концентрация полномочий) и оправдания (внутренняя рационализация, позволяющая лицу примирить свои действия с представлением о допустимом поведении). Для экономической разведки эта модель имеет непосредственное прикладное значение. Анализ давления позволяет выявить лиц и ситуации повышенного риска. Анализ возможностей указывает на организационные уязвимости, которые могут быть использованы для совершения злоупотреблений. Оценка распространенности оправдательных установок характеризует этический климат в организации и помогает определить приоритеты профилактической работы.

Характерные схемы корпоративного мошенничества в российских компаниях включают несколько устойчивых моделей, воспроизводящихся в различных отраслях. Закупочное мошенничество предполагает сговор должностного лица, ответственного за закупки, с поставщиком. Механизм сговора может включать завышение закупочных цен с последующим разделением разницы, оплату фактически не поставленных материалов на основании фиктивных накладных, систематическую подмену качественного сырья некондиционным при оплате по полной стоимости. Платежное мошенничество включает перенаправление денежных средств на подставные организации через подмену реквизитов, оплату фиктивных услуг на основании сфабрикованных актов, использование дробления платежей для обхода контрольных лимитов. Мошенничество с активами охватывает присвоение имущества, нецелевое использование корпоративных средств. Мошенничество с отчетностью направлено на искажение финансового состояния организации: завышение выручки, занижение расходов, неотражение обязательств, манипулирование резервами, досрочное признание доходов.

Внешние угрозы в российской деловой среде приобрели особую значимость после 2014 года и существенно обострились после 2022 года. Санкционные ограничения затронули платежную инфраструктуру, ограничили доступ к отдельным рынкам капитала, изменили структуру контрагентских связей и создали необходимость перестройки логистических маршрутов. Руководство Европейской комиссии по усиленной проверке контрагентов (Guidance for EU operators, 2023) прямо указало на необходимость расширенного анализа деловых партнеров и бенефициарных владельцев в контексте обхода ограничительных мер [47]. Для российских компаний это означает, что проверка контрагента должна охватывать структуру владения, аффилированность, санкционную историю и поведение в расчетах – информацию, далеко выходящую за пределы стандартного запроса бухгалтерской отчетности.

Перестройка платежных маршрутов после 2022 года создала новые уязвимости. Использование ранее незнакомых финансовых посредников повысило вероятность мошенничества

со стороны третьих лиц. Переход на расчеты в национальных валютах потребовал пересмотра процедур хеджирования валютных рисков. Ограничения корреспондентских отношений банков увеличили время проведения платежей и расширили круг промежуточных участников, каждый из которых представляет потенциальную точку уязвимости. Рекомендации FATF (2012, с изменениями на 2025 год) предусматривают применение усиленной проверки клиентов и контрагентов при повышенном уровне риска [34]. Обзоры финансовой стабильности Банка России фиксируют системные уязвимости финансового сектора и формулируют рекомендации по их устранению [25].

Цифровые угрозы стали самостоятельной группой по мере перевода финансовых операций в электронную среду. Подмена платежных реквизитов через компрометацию электронной почты (так называемая атака business email compromise), перехват электронной переписки с банковскими инструкциями, компрометация учетных записей в системах дистанционного банковского обслуживания, применение методов социальной инженерии для получения доступа к финансовым данным, внедрение программ-вымогателей, блокирующих доступ к корпоративным данным, – все это образует класс угроз, требующих согласованных усилий финансовой службы и подразделения информационной безопасности.

Cheng, Zou, Xiang и Jiang (2025) обобщили применение графовых нейронных сетей для обнаружения мошеннических транзакций и показали, что подобные модели способны выявлять скрытые закономерности, недоступные традиционным аналитическим методам. Авторы подчеркнули, что для эффективного применения требуются качественные обучающие данные и регулярная переобучение моделей с учетом изменяющихся схем мошенничества [48]. При этом NIST AI 100—2e2025 предупреждает о рисках атак на сами системы машинного обучения, включая отравление обучающих данных (data poisoning) и обход классификаторов (evasion attacks). Для компаний, внедряющих подобные решения, это означает необходимость обеспечения безопасности не только анализируемых данных, но и самой аналитической инфраструктуры [49].

ISO/IEC 27001:2022 задает требования к системе управления информационной безопасностью, определяя порядок оценки рисков, выбора мер защиты и мониторинга их эффективности [19]. ГОСТ Р 57580.1—2017 содержит базовый состав организационных и технических мер защиты информации финансовых организаций, включая требования к контролю доступа, регистрации событий безопасности и защите данных при передаче [20]. Положения 187-ФЗ о критической информационной инфраструктуре устанавливает дополнительные требования для организаций, нарушение функционирования информационных систем которых может повлечь существенные последствия [18].

Механизм трансформации потенциальной угрозы в реальный ущерб включает несколько последовательных стадий, между которыми существуют временные интервалы, создающие пространство для раннего выявления и пресечения. На первой стадии существует источник опасности – внутренний (должностное лицо, имеющее мотив и возможность для злоупотребления) или внешний (недобросовестный контрагент, мошенническая организация, хакерская группа). На второй стадии источник получает доступ к уязвимой процедуре: незащищенному платежному каналу, должностному лицу с избыточными полномочиями, контрагенту, чья благонадежность не подтверждена надлежащей проверкой. На третьей стадии происходит реализация воздействия – совершается действие, направленное на причинение ущерба или извлечение неправомерной выгоды. На четвертой стадии проявляются последствия: прямые финансовые потери, искажение учетных данных, нарушение обязательств, утрата деловой репутации, судебные разбирательства.


Рисунок 4 – Механизм трансформации угрозы в ущерб

*Источник: составлено автором.*

Рисунок 4 наглядно показывает последовательность стадий от источника опасности до наступления последствий. Между второй и третьей стадиями обозначено пространство для раннего выявления – именно здесь экономическая разведка имеет наибольшие возможности для предупреждения ущерба. Если источник активен, но уязвимость отсутствует (мошенник пытается подменить реквизиты, однако платежная система автоматически сверяет данные с реестром), угроза не реализуется. Если уязвимость существует, но источник неактивен, она остается латентной. Задача экономической разведки – обнаруживать как источники, так и уязвимости до того, как они совпадут в одной операции.

Отраслевая специфика финансовых угроз оказывает существенное влияние на их состав, приоритетность и методы выявления. Производственные предприятия подвержены угрозам в области закупочной деятельности: завышение цен на сырье и комплектующие, фиктивные поставки, подмена материалов, сговор закупщика с поставщиком. Торговые организации сталкиваются с угрозами в области управления дебиторской задолженностью, ценообразования и контроля товарных запасов. Строительные компании подвержены угрозам завышения сметной стоимости, фиктивного выполнения работ и отвлечения средств целевого финансирования. Финансовые организации имеют специфический набор угроз, связанных с кредитным, операционным и регуляторным рисками. Компании, работающие с государственными контрактами, испытывают повышенную зависимость от единственного заказчика, что создает уязвимость к задержкам бюджетного финансирования и односторонним изменениям условий.

Информационная асимметрия выступает фактором, общим для всех категорий угроз. Компания располагает полными сведениями о собственных операциях, но в отношении контрагентов вынуждена опираться на ограниченные данные: публичную отчетность, данные государственных реестров, информацию из открытых источников и сведения, добровольно предоставляемые самим контрагентом. Качество этих данных варьируется: публичная отчетность может быть составлена формально, реестровые данные – устареть, а сведения от контрагента – оказаться неполными или недостоверными. Экономическая разведка направлена на сокращение информационной асимметрии путем целенаправленного сбора и перекрестной проверки данных из нескольких независимых источников.

Sorensen (2025) рассмотрел методы скрининга корпоративного управления и анализа негативных информационных сигналов (adverse media screening) для выявления корпоративного мошенничества. Автор указал на информативность таких показателей, как концентрация управленческой власти, качество работы аудиторского комитета, частота смены аудиторов и наличие повторяющихся обращений в суд со стороны одних и тех же контрагентов [46].

Ionescu, Dumitrescu, Ioanas и Delcea (2024) провели библиометрический анализ публикаций по приоритетным показателям деятельности и риска, установив растущий интерес к интеграции этих показателей в единую управленческую систему, что подтверждает тенденцию к сближению финансового анализа и анализа угроз [10].

Завершая подглаву, зафиксируем основные положения. Финансовые угрозы носят многофакторный характер и классифицируются по источнику (внутренние, внешние, цифровые, мошеннические) и по механизму реализации (прямое воздействие, искажение информации, нарушение порядка решений, воспрепятствование контролю). Угроза всегда предполагает наличие источника и уязвимости; при отсутствии одного из элементов она не реализуется. Механизм трансформации угрозы в ущерб проходит через несколько стадий, между которыми существует пространство для раннего выявления. Именно на это пространство направлена деятельность экономической разведки.

## 1.3. Методологические подходы к оценке финансовой безопасности

Оценка финансовой безопасности компании представляет собой систематическое установление того, в какой мере финансовое состояние и финансовые процессы организации способны противостоять воздействию внутренних и внешних угроз, описанных в предыдущем подглаве. Содержательное отличие оценки от текущего контроля состоит в горизонте анализа и характере выводов. Контроль фиксирует соблюдение процедур и лимитов по отдельным операциям здесь и сейчас. Оценка устанавливает свойства финансовой системы компании в целом: ее уязвимости, чувствительность к изменениям среды и достаточность защитных мер для поддержания платежеспособности и сохранения стоимости активов на обозримом горизонте [1, 2].

Выбор методологического подхода определяется целью управленческого решения, доступностью данных и требуемой воспроизводимостью выводов. В научной и профессиональной литературе представлены несколько устоявшихся подходов: индикаторный, интегрально-индексный, рейтинговый (банковского типа), сбалансированный (включающий нефинансовые факторы), риск-ориентированный и балльно-рейтинговый. Каждый из них обладает собственными достоинствами и ограничениями, которые рассмотрены ниже.

Индикаторный подход основан на системе количественных и качественно определяемых показателей, отражающих состояние финансовой безопасности через наблюдаемые признаки устойчивости и защищенности. Индикатор выступает как наблюдаемая величина, связанная с угрозой, уязвимостью или последствием. Его ценность – в возможности регулярного наблюдения за изменением состояния и сопоставления периодов. Методика индикаторной оценки включает несколько последовательных этапов: определение состава угроз и уязвимостей, выбор показателей, установление правил расчета и источников данных, задание пороговых значений и зон состояния, закрепление порядка действий при выходе показателя за пределы нормы [3, 27].

Сила индикаторного подхода – в воспроизводимости результата. Если правила расчета зафиксированы и данные берутся из учетных систем, результат может быть повторен независимым специалистом. Это создает основу для межпериодного сопоставления и для использования в качестве доказательства при обосновании управленческих решений. Ограничение состоит в том, что индикатор по определению фиксирует уже наблюдаемое состояние, но может запаздывать по отношению к формирующейся угрозе: ухудшение ликвидности отражается в отчетности лишь после того, как событие, его вызвавшее, уже произошло. Кроме того, индикатор зависит от качества учетных данных и может быть искажен при ненадлежащем ведении учета.

Среди классических индикаторных инструментов заслуживают внимания модели прогнозирования финансовой несостоятельности. Модель Altman (1968) основана на пяти финансовых коэффициентах: отношении рабочего капитала к активам, нераспределенной прибыли к активам, прибыли до уплаты процентов и налогов к активам, рыночной стоимости собственного капитала к обязательствам и выручки к активам. Итоговый показатель Z-score рассчитывается как линейная комбинация этих коэффициентов с фиксированными весами и позволяет отнести компанию к зоне благополучия, неопределенности или вероятного банкротства [41]. Beaver (1966) показал предсказательную способность отдельных финансовых коэффициентов, в частности отношения денежного потока к обязательствам, за пять лет до наступления несостоятельности [42]. Ohlson (1980) предложил вероятностный подход на основе логистической регрессии, позволяющий учитывать размер компании и направление изменения показателей [43].

Данные модели разрабатывались для условий развитого рынка и требуют адаптации к российской специфике. Различия в стандартах бухгалтерского учета, в отраслевой структуре экономики, в ликвидности фондового рынка и в доступности данных означают, что прямое применение коэффициентов Altman к российской компании может дать некорректный результат. Рыночная стоимость собственного капитала, входящая в четвертый коэффициент, для непубличных компаний (составляющих подавляющее большинство российских организаций) недоступна. Вместе с тем логика построения этих моделей – выделение наиболее значимых финансовых признаков ухудшения состояния и их объединение в предсказательную конструкцию – остается методически ценной.

Интегральные индексы позволяют свести разнородные показатели к единому значению, обеспечивая обобщенное представление о состоянии компании. Руководство OECD по построению составных индикаторов (Handbook on Constructing Composite Indicators, 2008) содержит рекомендации по выбору переменных, нормированию, взвешиванию и агрегированию, а также по анализу робастности итогового значения [27]. Данный документ выделяет десять последовательных этапов: формирование теоретической базы, выбор переменных, обработку пропущенных значений, многомерный анализ, нормирование, взвешивание, агрегирование, анализ устойчивости, связь с другими показателями и визуализацию результатов. Для корпоративной оценки безопасности наиболее существенными представляются этапы нормирования (приведение разнородных показателей к единой шкале), взвешивания (отражение относительной значимости компонентов) и анализа устойчивости (проверка чувствительности итогового значения к вариации отдельных параметров).

Ограничение интегральных индексов хорошо известно: при агрегировании утрачивается детальность. Две компании с одинаковым итоговым значением могут иметь принципиально различный профиль уязвимостей. Высокая ликвидность может маскировать слабую своевременность платежей, а надежные процедуры контроля – сосуществовать с критической зависимостью от единственного контрагента. По этой причине любой интегральный показатель должен сопровождаться возможностью декомпозиции: от итогового значения к групповым оценкам, а от них – к отдельным индикаторам, указывающим на конкретный источник уязвимости.

Банковские рейтинговые системы, прежде всего CAMELS (Capital adequacy, Asset quality, Management, Earnings, Liquidity, Sensitivity to market risk), представляют интерес для корпоративного анализа, несмотря на изначальную ориентацию на кредитные организации. Руководство FDIC по экзаменационной политике (Risk Management Manual, 2025) детально описывает процедуру присвоения оценок по каждому компоненту системы и порядок формирования итоговой рейтинговой оценки [28]. Достоинство CAMELS – в ее структурированности и апробированности: система используется в банковском надзоре десятилетиями и прошла многочисленные проверки практикой. Ее адаптация к нефинансовой компании, однако, требует существенного пересмотра содержания отдельных блоков. Компонент S (чувствительность к рыночному риску) для производственной организации проявляется через зависимость от валютного курса, стоимости сырья и условий заемного финансирования,, в отличие от через позиции по процентным ставкам и валютным деривативам, как в банке.

Сбалансированная система показателей (Balanced Scorecard), предложенная Kaplan и Norton (1996), позволяет включить в оценку нефинансовые факторы: качество внутренних процессов, состояние информационных систем, квалификацию персонала и клиентскую перспективу [29]. Для целей финансовой безопасности ценность данного подхода заключается в возможности учитывать опережающие индикаторы – признаки, которые предшествуют ухудшению финансового состояния и позволяют принять решение до наступления потерь. Ухудшение качества внутренних процессов (рост числа ошибок при согласовании, увеличение задержек, пропуск контрольных процедур) может предвещать финансовое ухудшение задолго до его

отражения в отчетности. Ограничение сбалансированной системы – в высокой трудоемкости настройки и в зависимости от субъективных суждений при определении каузальных связей между перспективами.

Риск-ориентированный подход, закрепленный в международном стандарте ISO 31000:2018, документах COSO Enterprise Risk Management (2017) и руководстве COSO и ACFE по управлению рисками мошенничества (2023), рассматривает безопасность через призму систематического управления рисками [24, 26, 52]. ISO 31000:2018 определяет риск как эффект неопределенности в отношении целей и предлагает процессную модель, включающую установление контекста, идентификацию, анализ, оценку и обработку рисков. COSO ERM (2017) расширяет модель, связывая управление рисками со стратегией и операционной деятельностью организации. Для экономической разведки данный подход создает методическую основу, поскольку устанавливает последовательность действий от обнаружения сигнала до проверки эффекта принятого решения.

Балльно-рейтинговые модели выступают как инструмент формализации экспертных оценок при ограниченной статистической базе. Городецкая (2022) применила балльно-рейтинговый подход для оценки проблем экономической безопасности в учетно-аналитической системе организации, показав возможность количественного сопоставления разнородных факторов [17 по оригиналу]. Beasley, Branson и Hancock (2010) обосновали подход к разработке приоритетных индикаторов риска (KRI) для целей корпоративного управления рисками, продемонстрировав, что KRI способны предупреждать о нарастании угрозы до ее реализации [40]. Mekimah, Zighed, Mili и Bengana (2024) провели библиометрический анализ публикаций по деловой аналитике и управленческим решениям, установив, что тема интеграции аналитических инструментов в процесс управления продолжает активно развиваться [44].


Рисунок 5 – Методологические подходы к оценке финансовой безопасности

*Источник: составлено автором.*

Рисунок 5 иллюстрирует соотношение рассмотренных методологических подходов. Каждый из них раскрывает определенную сторону финансовой безопасности: индикаторный подход дает количественное основание, интегральные индексы обеспечивают обобщение, рейтинговые модели – сопоставимость, сбалансированная система – включение нефинансовых факторов, риск-ориентированный подход – процедурную последовательность. Авторская методика, разрабатываемая во второй и третьей главах, объединяет элементы нескольких подходов в комбинированную модель оценки.

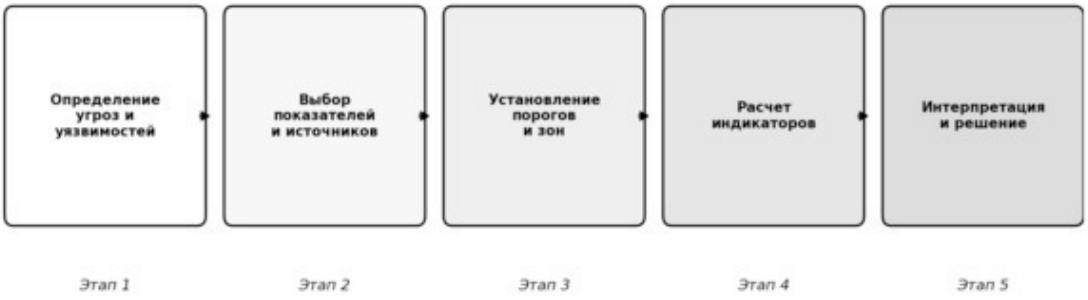


Рисунок 6 – Построение индикаторной системы безопасности

*Источник: составлено автором.*

Рисунок 6 отражает этапы построения индикаторной системы: от определения угроз и уязвимостей через выбор показателей и установление порогов к расчету индикаторов и принятию управленческого решения. Каждый индикатор связан с конкретной угрозой или уязвимостью, что обеспечивает адресность выводов.

Отдельного рассмотрения заслуживает обращение с пороговыми значениями и нормативами. Универсальные пороговые значения в корпоративных системах применимы ограниченно: различия отраслей, сезонности, инвестиционных циклов и структуры контрактов меняют содержание показателя. Коэффициент текущей ликвидности, равный 1,5, для торговой компании с быстрым оборотом может свидетельствовать о вполне удовлетворительном состоянии, тогда как для строительной организации с длительным производственным циклом аналогичное значение может указывать на недостаточность оборотных средств. Методика должна различать пороговые значения обязательного соблюдения, установленные законом или договором (ковенанты, нормативы достаточности капитала, условия раскрытия информации), и пороговые значения управленческого наблюдения, которые компания вводит самостоятельно для раннего обнаружения неблагоприятных изменений [2, 10, 25].

Методологические принципы оценки финансовой безопасности формируются из трех требований. Проверяемость означает, что используемые данные имеют установленный источник в учетной системе, управленческой отчетности или верифицированной внешней информации, а правила вычисления показателей зафиксированы и поддаются повторению. Сопоставимость требует единого определения показателей по периодам и подразделениям, а также учета изменений учетной политики и организационной структуры. Управленческая применимость означает, что итоговая оценка позволяет установить, какие уязвимости усиливают угрозы, и какие конкретные действия способны снизить вероятность ущерба [19, 24, 26].

Сравнительный анализ подходов позволяет выделить их относительные преимущества и ограничения. Индикаторный подход дает наиболее воспроизводимые результаты, но зависит от качества учетных данных и не учитывает факторы, не отраженные в отчетности. Интегральные индексы обеспечивают обобщение, но утрачивают детальность. Рейтинговые модели банковского типа хорошо структурированы, но требуют существенной адаптации к нефинансовому сектору. Сбалансированная система показателей позволяет включить нефинансовые факторы, но трудоемка в настройке и зависит от субъективности каузальных связей. Риск-ориентированный подход обеспечивает процедурную последовательность, но в российских условиях сталкивается с дефицитом данных для количественных оценок вероятности.

По этой причине в настоящей работе предпочтение отдано комбинированному подходу. Для оценки конкретной угрозы предлагается пятипараметрический индекс (ИФУН), использующий экспертно-балльную шкалу и учитывающий вероятность реализации, уязвимость процедуры, масштаб возможного ущерба, качество раннего выявления и необратимость последствий. Для обобщенной оценки состояния компании предлагается коэффициент уровня экономической безопасности (КУЭБ), объединяющий групповые оценки с возможностью декомпозиции до уровня отдельных показателей. Дополнительно предлагаются коэффициент межугрозового усиления (КМУ), отражающий каскадное взаимодействие между одновременно действующими угрозами, и коэффициент латентности (Кл), измеряющий продолжительность скрытого периода угрозы. Обоснование формул, шкал, весов и порядка расчета этих инструментов составляет предмет второй и третьей глав.

Развитие концепции экономической безопасности в российской науке не было однородным. К настоящему времени сложились несколько исследовательских направлений, различающихся по расстановке акцентов, методологическим приоритетам и прикладной ориентации. Первое направление, представленное работами Института экономики РАН, тяготеет к макроэкономическому анализу и акцентирует внимание на роли государственного регулирования, защите стратегических отраслей и обеспечении технологического суверенитета. Второе направление, развиваемое в финансовых университетах и академиях, сосредоточено на финансовых аспектах безопасности предприятий: ликвидности, доходности, долговой нагрузке и защите от финансовых потерь. Третье направление, формирующееся на стыке экономической науки и информационной безопасности, рассматривает защиту корпоративной информации как неотъемлемый компонент экономической безопасности.

Каждое из этих направлений внесло определенный вклад в формирование современного понимания предмета. Макроэкономический подход обеспечил связь корпоративного уровня с государственными приоритетами и позволил сформулировать индикаторные системы, пригодные для мониторинга состояния отраслей и секторов. Финансовый подход предоставил инструментарий количественной оценки, основанный на бухгалтерской отчетности и финансовых коэффициентах. Информационный подход привлек внимание к роли данных, информационных систем и цифровых технологий в обеспечении безопасности. Ограничение каждого из подходов, взятого в отдельности, состоит в неполноте охвата: макроэкономический подход не учитывает управленческую специфику организации, финансовый – недостаточно внимания уделяет качеству процедур и информационной среде, информационный – не связан с финансовыми показателями и управленческими решениями.

В настоящей работе предпринимается попытка соединить элементы перечисленных подходов применительно к конкретной задаче – организации экономической разведки для предупреждения финансового ущерба. Такое соединение обусловлено природой предмета: финансовая угроза одновременно представляет собой экономическое явление, правовой факт, управленческую проблему и информационное событие. Ее исследование невозможно средствами одной лишь финансовой аналитики; оно требует привлечения правовой информации, данных об организационных процессах и сведений из открытых источников.

Международный контекст развития концепции корпоративной безопасности определяется работами по корпоративному управлению, управлению рисками и противодействию мошенничеству. Принципы G20/OECD Principles of Corporate Governance (2023) формулируют общие ожидания в отношении качества корпоративного управления, включая защиту прав акционеров, раскрытие информации и подотчетность совета директоров [50]. Модель COSO ERM (2017) задает процессную модель управления рисками, связанную со стратегическими целями организации [26]. Модель COSO (2013) определяет компоненты системы внутреннего контроля и порядок оценки их эффективности [33]. COSO и ACFE Fraud Risk Management Guide (2023) содержит рекомендации по управлению рисками мошенничества, включая оценку предрасположенности организации к мошенническим действиям [52]. IFC Internal Control Handbook (2021) предоставляет практические инструменты для организаций различного масштаба, включая шаблоны политик и процедур [51].

Для российской науки характерно стремление синтезировать отечественный и зарубежный опыт, адаптируя международные стандарты и рекомендации к условиям российской правовой и институциональной среды. Подобная адаптация необходима, поскольку прямое заимствование иностранных моделей без учета специфики российского делового оборота нередко приводит к формальному копированию, в отличие от содержательного применения заимствованных инструментов. Качественная адаптация требует понимания как возможностей, так и ограничений заимствуемых подходов, а также готовности к их модификации с учетом конкретных условий применения.

Для российских компаний среднего масштаба наиболее характерны несколько категорий внутренних финансовых потерь. Переплата при закупке сырья и материалов возникает вследствие отсутствия конкурентного отбора поставщиков или сговора закупщика с поставщиком. Потери от несвоевременных расчетов приводят к штрафным санкциям и утрате скидок за раннюю оплату. Потери от неправомерного использования корпоративных средств должностными лицами включают необоснованные командировочные расходы, использование корпоративных ресурсов в личных целях, оплату услуг, оказанных аффилированными организациями по завышенным ценам. Потери от невозврата авансов возникают при работе с недобросовестными подрядчиками, которые получают предварительную оплату, но не исполняют обязательства. Каждый из перечисленных видов потерь имеет собственный механизм реализации и требует специфических методов выявления: сопоставления закупочных цен с рыночными, анализа своевременности платежей, проверки обоснованности расходов, оценки надежности подрядчиков.

Признаки мошенничества (так называемые красные флаги, или настораживающие индикаторы) систематизированы в профессиональной литературе и стандартах аудита. К наиболее распространенным признакам относятся: необъяснимый рост расходов при стабильных или снижающихся объемах деятельности; систематическое дробление сумм чуть ниже порога обязательного согласования; частые изменения поставщиков без объективных хозяйственных причин; совпадение адресов, телефонов или учредителей у нескольких контрагентов; устойчивое несоответствие между данными управленческого и бухгалтерского учета; сопротивление проверкам со стороны должностных лиц; нетипичный образ жизни работника при невысоком должностном окладе; отказ от отпуска (предотвращающий временную передачу функций другому лицу и, соответственно, обнаружение нарушений).

Методы выявления мошенничества включают аналитические процедуры (анализ отклонений, сопоставление данных из нескольких источников, проверка нетипичных операций, применение закона Бенфорда для обнаружения аномалий в распределении первых цифр сумм), процедурные проверки (пересчет, инвентаризация, сверка с контрагентами, подтверждение внешних данных), а также информационные методы (анализ открытых источников, проверка аффилированности, мониторинг судебных дел). Для экономической разведки существенно,

что эффективное выявление требует сочетания нескольких методов: аналитическая процедура может указать на аномалию, но для подтверждения или опровержения мошеннической природы необходима дополнительная проверка, включающая документальное подтверждение и, нередко, получение сведений из внешних источников.

Конфликт интересов занимает промежуточное положение между мошенничеством и управленческой ошибкой. Должностное лицо, заключающее договор с организацией, в которой оно имеет скрытый финансовый интерес, действует в ущерб представляемой компании, даже если условия договора формально соответствуют рыночным. Для экономической разведки выявление конфликтов интересов представляет особую трудность, поскольку аффилированность может быть замаскирована через цепочку юридических лиц, доверительное управление, использование номинальных учредителей или неформальные договоренности. Sorensen (2025) указал на информативность показателей концентрации управленческой власти и качества работы аудиторского комитета для выявления предпосылок корпоративного мошенничества [46].

Согласование терминов финансовой устойчивости и финансовой безопасности имеет принципиальное значение для построения методики оценки. Финансовая устойчивость описывает способность организации поддерживать платежеспособность и приемлемую структуру источников финансирования при неблагоприятных воздействиях, сохраняя возможность воспроизводства капитала. Финансовая безопасность по содержанию шире: она включает защиту финансовых интересов организации, устойчивость финансовых процессов, достоверность финансовой информации и способность противостоять умышленным воздействиям, включая мошенничество, манипулирование данными и вмешательство в платежные процедуры. Методика оценки финансовой безопасности, следовательно, должна включать элементы оценки устойчивости (финансовые коэффициенты), оценки защищенности процессов (качество процедур контроля) и оценки качества финансовой информации (достоверность учетных данных). Брагина и Круц (2023) обосновали подобное расширенное понимание, указав на необходимость выхода за пределы традиционного финансового анализа [15].

Для полноты сравнительного анализа укажем на метод FMEA (Failure Mode and Effects Analysis – анализ видов и последствий отказов), первоначально разработанный для инженерных целей. Метод предполагает расчет приоритетного числа риска (Risk Priority Number, RPN) как произведения трех параметров: серьезности последствий (Severity), вероятности возникновения (Occurrence) и способности обнаружения (Detection). Итоговый показатель RPN = S x O x D используется для ранжирования рисков и определения приоритетов корректирующих действий. Авторский индекс ИФУН, разрабатываемый во второй главе, имеет определенное структурное сходство с FMEA, однако существенно отличается от него по нескольким позициям: включает уязвимость процедуры как самостоятельный параметр (а не часть вероятности), выделяет необратимость последствий в отдельный множитель и дополнен коэффициентом межугрозового усиления, отражающим каскадное взаимодействие между одновременно действующими угрозами. Данные отличия обусловлены спецификой корпоративных финансовых угроз, которые, в отличие от инженерных отказов, нередко носят преднамеренный характер и способны усиливать друг друга.

В качестве дополнительного аргумента в пользу комбинированного подхода укажем на наблюдение Ionescu, Dumitrescu, Ioanas и Delcea (2024), которые в библиометрическом исследовании приоритетных показателей деятельности и риска обнаружили устойчивую тенденцию к интеграции количественных и качественных методов оценки. Авторы показали, что публикации последних лет все чаще сочетают финансовые индикаторы с оценкой процессов, организационной культуры и качества управления, что свидетельствует о формирующемся консенсусе в пользу многоаспектной оценки безопасности [10].

Вопрос о периодичности оценки имеет практическое значение. Излишне частая оценка (ежедневная, еженедельная) перегружает аналитическую функцию и порождает информационный шум, затрудняющий выделение действительно существенных изменений. Излишне редкая оценка (ежегодная) рискует пропустить нарастание угрозы, которое в промежутке между проверками может перейти в стадию реализации. Для большинства компаний среднего масштаба оптимальной представляется ежеквартальная оценка коэффициента КУЭБ с возможностью внеочередного расчета при наступлении существенных событий (крупные сделки, изменение структуры контрагентов, цифровые инциденты, санкционные изменения). Расчет индекса ИФУН целесообразно проводить при каждом обнаружении потенциальной угрозы, то есть по мере поступления сигналов.

Принципиальное ограничение, общее для всех рассмотренных подходов, состоит в зависимости от полноты и достоверности исходных данных. Качество оценки определяется не столько сложностью применяемых формул, сколько надежностью информационной базы, на которой эти формулы работают. Если бухгалтерская отчетность не отражает действительного финансового положения (вследствие ошибок или умышленного искажения), финансовые коэффициенты утрачивают информативность. Если проверка контрагентов проводится формально и не включает сопоставление данных из нескольких независимых источников, ее результаты ненадежны. Если управленческая отчетность составляется с опозданием, оценка безопасности оперирует устаревшими данными. По этой причине в последующих главах для каждого параметра предложенных индексов будут установлены конкретные требования к источникам данных и документальному подтверждению присвоенных значений.

Формирование экономической разведки как корпоративной функции в российских условиях существенно отличается от западного опыта. В странах англосаксонской правовой традиции корпоративные расследования и проверки деловых партнеров (due diligence) имеют развитую правовую и методическую базу: судебная практика, профессиональные стандарты (в частности, стандарты Международной ассоциации сертифицированных исследователей мошенничества – ACFE), нормативные ожидания регуляторов создают устойчивую среду для аналитической работы. В России подобная среда еще находится в стадии формирования. Отечественные компании нередко организуют аналитическую функцию по собственному усмотрению, без четкого методического ориентира, что приводит к значительному разбросу в качестве получаемых результатов.

Содержание работы экономической разведки можно структурировать по нескольким направлениям. Первое – проверка контрагентов: сбор и анализ сведений о деловых партнерах для оценки их финансовой состоятельности, благонадежности и соответствия установленным требованиям. Второе – мониторинг финансовых операций: наблюдение за движением денежных средств, выявление нетипичных транзакций, контроль за соблюдением лимитов и процедур согласования. Третье – анализ внешней среды: отслеживание изменений нормативного регулирования, санкционных списков, рыночных условий и действий конкурентов, имеющих значение для финансовой безопасности компании. Четвертое – внутренняя аналитика: выявление признаков злоупотреблений, конфликтов интересов и процедурных нарушений на основе анализа внутренних данных. Пятое – подготовка аналитических заключений: формирование выводов, рекомендаций и материалов для принятия управленческих решений.

Каждое из перечисленных направлений предъявляет собственные требования к квалификации исполнителей, источникам данных и методам анализа. Проверка контрагентов требует навыков работы с открытыми реестрами, судебными базами данных, отраслевыми источниками и специализированными информационными системами (СПАРК, Фокус и аналоги). Мониторинг финансовых операций основан на данных бухгалтерского и управленческого учета и предполагает владение методами финансового анализа. Анализ внешней среды требует понимания нормативного поля, в том числе международных ограничительных мер.

Внутренняя аналитика предполагает доступ к кадровым данным, договорной документации и корпоративной переписке. Подготовка заключений требует умения формулировать выводы в форме, пригодной для руководства: ясно, обоснованно, с указанием степени подтвержденности и предложений по действию.

Федеральный государственный образовательный стандарт по специальности 38.05.01 «Экономическая безопасность» (приказ Минобрнауки от 14.04.2021 No 293) предусматривает формирование компетенций в области финансового анализа, контроля, аудита и противодействия правонарушениям в сфере экономики [54]. Вместе с тем практические навыки работы с конкретными угрозами, проверки контрагентов в условиях санкционных ограничений, применения цифровых инструментов анализа данных приобретаются преимущественно в ходе профессиональной деятельности и дополнительного образования. Momeni и Behnampour (2026) исследовали содержание учебных программ по forensic accounting в северо-американских университетах и установили, что наиболее эффективные курсы сочетают теоретическую подготовку с анализом реальных кейсов и практической работой с документами [56]. Okougbo, Okike и Alao (2021) показали, что включение модулей по этике бухгалтерского учета повышает этическую осведомленность студентов, что существенно для формирования профессиональной культуры работы с чувствительной информацией [57].

Значение кадрового обеспечения для экономической разведки трудно переоценить. Самые совершенные процедуры и информационные системы утрачивают ценность, если исполнители не обладают необходимой квалификацией, не понимают смысла выполняемых действий или относятся к ним формально. Bracewell и Jones (2022) обосновали эффективность использования симуляций криминалистических ситуаций в обучении, показав, что активные методы повышают качество усвоения практических навыков [58]. Shillair и соавторы (2022) обобщили национальный опыт программ повышения осведомленности в области кибербезопасности и установили, что регулярные тренировки значительно эффективнее формальных инструктажей [59]. Hillman, Harel и Toch (2023) оценили программы противодействия фишингу на уровне крупной организации и показали, что сочетание обучения с имитационными проверками снижает долю работников, реагирующих на мошеннические сообщения [60].

Связь финансовых угроз с платежным порядком заслуживает более подробного рассмотрения. Платежный порядок отражает своевременность и полноту исполнения денежных обязательств, а также надежность применяемых платежных процедур. Ее ухудшение может быть как следствием финансовых затруднений контрагента, так и результатом преднамеренных действий. Задержка платежей, частичное исполнение обязательств, необоснованное изменение платежных реквизитов, настойчивые требования ускоренного платежа без надлежащего документального подтверждения – каждое из этих обстоятельств может служить ранним сигналом неблагоприятного развития событий. Для экономической разведки платежный порядок выступает одновременно объектом наблюдения и источником сигналов.

Особого внимания заслуживает проблема манипулирования платежными реквизитами. Подмена реквизитов контрагента с целью перенаправления платежа на счет злоумышленника относится к числу наиболее распространенных схем внешнего мошенничества. Механизм атаки, как правило, включает компрометацию электронной почты контрагента или сотрудника компании, подготовку поддельного письма с указанием новых реквизитов и побуждение финансовой службы к перечислению средств на подставной счет. Защита от подобных атак предполагает обязательную верификацию любых изменений реквизитов через независимый канал связи (телефонный звонок по заранее известному номеру, личное подтверждение), а также автоматическую регистрацию всех изменений в справочнике контрагентов с уведомлением ответственных лиц.

Зависимость компании от ограниченного числа контрагентов создает специфическую уязвимость, которую целесообразно выделять в самостоятельную категорию. Если более двадцати процентов выручки приходится на одного покупателя или более тридцати процентов закупок – на одного поставщика, утрата данного контрагента способна привести к существенному ухудшению финансового положения. Для оценки данной уязвимости может применяться адаптированный индекс концентрации, аналогичный по конструкции индексу Херфиндаля-Хиршмана: чем выше значение индекса, тем выше концентрация и, соответственно, выше уязвимость компании к потере приоритетного партнера. Экономическая разведка должна включать регулярный мониторинг состояния основных контрагентов и раннее обнаружение признаков ухудшения их финансового положения или деловой надежности.

Угрозы, связанные с конфиденциальностью коммерческой информации, приобретают дополнительное значение в условиях цифровизации. Утечка сведений о планируемых сделках, ценовых условиях, технологических решениях или финансовом состоянии компании способна причинить ущерб, сопоставимый с прямыми финансовыми потерями. Законодательство о коммерческой тайне (98-ФЗ) определяет условия установления режима коммерческой тайны и ответственность за его нарушение [30]. Для экономической разведки защита собственной чувствительной информации представляет собой необходимое условие результативной работы: если аналитические выводы, материалы проверок или сведения о выявленных угрозах становятся доступны заинтересованным лицам, эффективность всей системы защиты ставится под сомнение.

При анализе каждого методологического подхода необходимо учитывать и организационные условия его применения. Индикаторный подход требует налаженной системы сбора данных и четких регламентов расчета. Интегральные индексы нуждаются в согласованной системе весов, что предполагает экспертное обсуждение и утверждение руководством. Рейтинговые модели требуют квалифицированных оценщиков, владеющих методикой присвоения баллов. Сбалансированная система показателей предполагает определение каузальных связей между перспективами, что является нетривиальной управленческой задачей. Риск-ориентированный подход нуждается в реестре рисков и процедуре его регулярного обновления.

Применимость каждого подхода зависит также от масштаба организации. Крупные компании с развитой аналитической инфраструктурой могут одновременно применять несколько методов, дополняющих друг друга. Для компаний среднего масштаба, располагающих ограниченными ресурсами, целесообразно выбрать комбинированный подход, совмещающий элементы индикаторной оценки (для мониторинга финансового состояния), балльно-рейтинговой оценки (для анализа конкретных угроз) и процедурного контроля (для обеспечения надежности чувствительных операций). Именно такой комбинированный подход реализован в авторской методике, представленной во второй и третьей главах.

Связь оценки финансовой безопасности с корпоративным управлением определяется тем, что результаты оценки должны быть встроены в процесс принятия решений. Оценка, результаты которой не доводятся до лиц, принимающих решения, или доводятся с существенным запозданием, утрачивает управленческую ценность. Принципы G20/OECD (2023) подчеркивают ответственность совета директоров за контроль системы управления рисками и внутреннего контроля [50]. IFC Internal Control Handbook (2021) содержит практические рекомендации по включению результатов оценки в повестку заседаний руководящих органов компании [51]. Для экономической разведки это означает необходимость разработки формата представления результатов, понятного и полезного для руководства: краткого, обоснованного, с четким указанием на выявленные проблемы и предложения по действию.

Вопрос об объективности и субъективности оценки заслуживает прямого рассмотрения. Любая оценка финансовой безопасности содержит элемент субъективности: в выборе показателей, в установлении пороговых значений, в определении весов, в присвоении балльных

оценок качественным параметрам. Полностью устранить субъективность невозможно и, по-видимому, не нужно: экспертное суждение остается незаменимым при оценке ситуаций, для которых отсутствуют статистические данные. Задача состоит не в устранении субъективности, а в ее ограничении и контроле: через фиксирование правил присвоения значений, через требование документального подтверждения каждой оценки, через независимую перепроверку результатов и через анализ устойчивости итоговых выводов к вариации отдельных параметров. Именно этот принцип положен в основу авторской методики.

Процессный подход к оценке безопасности предполагает рассмотрение оценки не как разового мероприятия, а как регулярного цикла: планирование оценки (определение целей, объема, периода), сбор данных (из учетных систем, от подразделений, из внешних источников), расчет показателей (по установленным правилам), интерпретация результатов (с учетом отраслевого контекста и текущих обстоятельств), подготовка заключения (для руководства), принятие решений (на основе заключения), контроль исполнения (проверка выполнения принятых решений), повторная оценка (для проверки эффекта принятых мер). Такая цикличность обеспечивает непрерывность наблюдения и позволяет отслеживать динамику состояния безопасности во времени.

Методические указания по оценке связаны с вопросом документирования. Каждый этап оценки должен быть документально зафиксирован: источники данных, расчеты, основания для присвоения значений, выводы и рекомендации. Документирование выполняет несколько функций: обеспечивает возможность повторной проверки (аудиторский след), позволяет привлечь к ответственности за ненадлежащее выполнение обязанностей, создает основу для накопления опыта и совершенствования методики, а также защищает аналитика от необоснованных претензий. В отечественной практике документирование нередко рассматривается как формальное требование; между тем его качество непосредственно влияет на достоверность и управленческую ценность оценки.

Экономическая разведка в корпоративном понимании решает несколько практических задач, которые определяют ее место в структуре управления. Первая задача – обеспечение информационной основы для выбора контрагентов. Прежде чем компания заключает договор с новым партнером, необходимо установить его правоспособность, финансовую состоятельность, деловую репутацию, наличие или отсутствие судебных разбирательств, структуру владения и возможную связь с лицами, находящимися под ограничительными мерами. Объем и глубина проверки должны соответствовать масштабу предполагаемой сделки и уровню риска: для разового мелкого заказа достаточно базовой проверки реестровых данных, для крупного долгосрочного контракта требуется расширенная проверка с анализом финансовой отчетности и структуры владения.

Вторая задача – мониторинг состояния действующих контрагентов. Первоначальная проверка фиксирует состояние партнера на момент заключения договора, однако это состояние может измениться в ходе исполнения обязательств. Ухудшение финансового положения контрагента, возбуждение судебных разбирательств, смена учредителей, внесение в санкционные списки, появление признаков процедуры банкротства – все это обстоятельства, которые должны отслеживаться на регулярной основе. Периодичность обновления сведений определяется масштабом операций с данным контрагентом и уровнем зависимости компании от его надлежащего поведения.

Третья задача – выявление и анализ подозрительных операций внутри компании. Аномальные изменения в структуре расходов, необъяснимые отклонения между плановыми и фактическими показателями, систематическое дробление платежей, нетипичные изменения в справочниках контрагентов, совпадение реквизитов нескольких получателей платежей – все это может служить признаком злоупотреблений или процедурных нарушений. Задача аналитика экономической разведки – не только зафиксировать аномалию, но и установить, явля-

ется ли она результатом ошибки, объективного изменения условий деятельности или преднамеренного действия.

Четвертая задача – подготовка аналитических материалов для управленческих решений. Результаты проверок и мониторинга должны быть представлены в форме, пригодной для использования руководством. Аналитическое заключение должно содержать: описание установленных фактов, оценку степени их подтвержденности (достоверно установлено, вероятно, требует дополнительной проверки), характеристику возможных последствий, предложение по способу реагирования и срок повторной проверки. Формулировки должны быть конкретными: общие указания на наличие рисков без привязки к конкретным обстоятельствам не могут служить основанием для управленческого решения.

Пятая задача – накопление аналитического опыта и совершенствование методики. Каждый рассмотренный эпизод – подтвержденный или опровергнутый – содержит информацию, полезную для будущей работы. Систематическое ведение реестра рассмотренных случаев позволяет выявлять повторяющиеся модели угроз, оценивать результативность принятых мер и корректировать критерии существенности. Подобное накопление опыта превращает экономическую разведку из реактивной функции, отвечающей на уже возникшие проблемы, в проактивную, предупреждающую формирование угроз на ранней стадии.

Место экономической разведки в организационной иерархии определяет ее независимость и результативность. Если аналитическая функция подчинена финансовому директору, возникает конфликт интересов при проверке финансовых операций. Если она входит в состав службы безопасности, аналитическая работа может подменяться оперативными методами, выходящими за пределы предмета настоящего исследования. Если аналитик подчинен руководителю того подразделения, деятельность которого подлежит проверке, независимость выводов ставится под сомнение. Оптимальным представляется подчинение непосредственно генеральному директору или комитету совета директоров по аудиту, что обеспечивает независимость аналитических выводов и прямой доступ к руководству для доклада о выявленных угрозах.

Санкционные ограничения образуют самостоятельную категорию финансовых угроз, существенно осложнившую деятельность российских компаний после 2022 года. Ограничение доступа к международным расчетным системам (прежде всего SWIFT), заморозка активов в иностранных юрисдикциях, запрет на отдельные виды сделок, требования усиленной проверки партнеров из определенных юрисдикций – все это создает условия, при которых компания может непреднамеренно оказаться вовлеченной в нарушение ограничительных мер. Последствия такого вовлечения включают блокировку платежей, заморозку активов, штрафные санкции и утрату деловых связей.

Методические указания ЕС по проверке контрагентов (Guidance for EU operators: Implementing enhanced due diligence to shield against Russia sanctions circumvention, 2023) прямо указывает на необходимость анализа конечных бенефициарных владельцев, структуры владения и контроля, географии операций и характера деловых связей [47]. Для российских компаний данные рекомендации имеют двоякое значение: с одной стороны, они определяют требования, которым должны соответствовать российские организации при работе с европейскими партнерами; с другой – они формулируют методические подходы к проверке контрагентов, которые могут быть использованы самими российскими компаниями при оценке надежности своих деловых партнеров.

Информационное обеспечение работы с санкционной проблематикой требует доступа к актуальным спискам ограничительных мер нескольких юрисдикций (в первую очередь ЕС, США, Великобритании, Канады и Австралии), регулярного обновления данных о структуре владения контрагентов, а также мониторинга изменений в законодательстве и правоприменительной практике. Для компаний, осуществляющих внешнеэкономическую деятельность, дан-

ная работа носит постоянный характер и требует специализированной квалификации. Ошибка в оценке санкционного статуса контрагента может привести к блокировке платежа, утрате товара и длительным судебным разбирательствам.

Фактор информационной асимметрии приобретает дополнительное значение в условиях перестройки контрагентских связей. Переход к работе с новыми партнерами, особенно из ранее непривычных юрисдикций, сопровождается повышенным уровнем неопределенности: информация о деловой репутации, финансовом состоянии и платежном порядке нового контрагента ограничена или недоступна. Экономическая разведка призвана сокращать эту неопределенность путем целенаправленного сбора и перекрестной проверки данных из нескольких независимых источников: открытых реестров юридических лиц соответствующей юрисдикции, международных баз данных деловой информации, банковских референций, отзывов иных партнеров, данных о судебных разбирательствах.

Построение системы индикаторов финансовой безопасности предполагает решение нескольких последовательных задач. Первая – определение состава угроз и уязвимостей, подлежащих наблюдению. Перечень угроз формируется на основании анализа хозяйственной деятельности компании, отраслевого опыта, нормативных требований и результатов предшествующих проверок. Вторая – выбор индикаторов, адекватно отражающих состояние каждой из выделенных угроз. Индикатор должен быть связан с угрозой содержательно (а не формально), иметь измеримый или ранжируемый характер и быть доступен для расчета на основании имеющихся данных. Третья – установление порогов и зон состояния. Порог определяет границу, при пересечении которой состояние считается изменившимся: от нормального к настораживающему, от настораживающего к критическому. Зоны позволяют классифицировать текущее значение показателя и определить требуемый уровень реагирования.

Четвертая задача – определение правил расчета и источников данных. Для каждого индикатора должны быть зафиксированы: формула расчета (или правила присвоения качественной оценки), периодичность расчета, источник исходных данных и ответственное лицо. Без подобной фиксации индикаторная система утрачивает воспроизводимость: различные исполнители могут рассчитывать один и тот же показатель по-разному, что обесценивает межпериодное сопоставление. Пятая задача – закрепление порядка действий при выходе показателя за пределы установленных норм. Если коэффициент текущей ликвидности опускается ниже порогового значения, кто должен быть уведомлен, в какой срок и какие действия предпринимаются? Без ответа на эти вопросы индикаторная система остается аналитическим упражнением, не встроенным в управленческий процесс.

Формирование весов при построении интегрального индекса представляет отдельную методическую проблему. Существуют три основных подхода к назначению весов: экспертный (веса определяются на основании суждения квалифицированных специалистов), статистический (веса выводятся из анализа данных, например, методом главных компонент) и равновесный (все компоненты получают одинаковый вес). Экспертный подход является наиболее распространенным в корпоративной практике, поскольку статистический требует значительного массива данных, который для задач оценки безопасности, как правило, недоступен. Равновесный подход представляет собой нижнюю границу обоснованности: он применяется при отсутствии содержательных оснований для дифференциации значимости компонентов, однако может привести к недооценке критически значимых факторов.

Анализ устойчивости (робастности) интегрального показателя позволяет установить, насколько итоговое значение чувствительно к изменению отдельных параметров. Руководство OECD (2008) рекомендует проводить анализ устойчивости по двум направлениям: чувствительность к изменению весов (как изменится ранжирование при других весах?) и чувствительность к изменению метода агрегирования (как изменится результат при замене аддитивной агрегации на мультипликативную?) [27]. Для авторской методики, разрабатываемой во второй

главе, анализ устойчивости будет проведен путем вариации значений отдельных параметров при фиксированных остальных, что позволит установить, какой параметр оказывает наибольшее влияние на итоговый индекс.

Необходимо также указать на связь методики оценки с принципами бухгалтерского учета и аудита. Федеральный закон от 06.12.2011 No 402-ФЗ о бухгалтерском учете устанавливает требования к полноте, достоверности и своевременности отражения фактов хозяйственной деятельности [22]. Международный стандарт аудита Пересмотренный ISA 240 (2025) определяет обязанности аудитора по выявлению рисков мошенничества [21]. Федеральный закон от 30.12.2008 No 307-ФЗ об аудиторской деятельности регламентирует порядок проведения аудита и использования его результатов [22]. Для экономической разведки данные нормативные акты определяют границы допустимого использования учетных данных и результатов аудита, а также устанавливают стандарты достоверности информации, на которых основывается оценка финансовой безопасности.

Применение моделей прогнозирования несостоятельности в российских условиях требует учета нескольких обстоятельств. Во-первых, модели Altman, Beaver и Ohlson разработаны на данных американских компаний середины и второй половины XX века; отраслевая структура, стандарты учета и макроэкономические условия существенно отличаются от современной российской среды. Во-вторых, для значительной части российских компаний (непубличных) недоступны рыночные данные (рыночная капитализация), входящие в формулу Z-score Altman. В-третьих, качество бухгалтерской отчетности российских организаций существенно различается: крупные публичные компании, составляющие отчетность по МСФО, обеспечивают более высокий уровень раскрытия, тогда как отчетность малых и средних организаций нередко отражает лишь минимально необходимый объем информации. Тем не менее принципы, заложенные в данные модели, – выделение наиболее значимых финансовых признаков ухудшения, их объединение в предсказательную конструкцию и проверка предсказательной способности на исторических данных – сохраняют методическую ценность [41, 42, 43].

Наумова и соавторы в серии публикаций (2018, 2019) предложили методику мониторинга финансовой безопасности хозяйствующего субъекта, основанную на оценке финансовых угрожающих рисков (financial threatening risks). Авторы разграничили текущие и потенциальные угрозы, предложили систему индикаторов для мониторинга каждой группы и обосновали периодичность оценки. Данная методика представляет интерес для настоящего исследования, поскольку она ориентирована на корпоративный уровень и учитывает специфику российской институциональной среды [6, 11].

Правовая среда экономической разведки в российской компании отличается от западных аналогов прежде всего отсутствием специального законодательного акта. В ряде зарубежных юрисдикций корпоративные расследования (corporate investigations) регулируются самостоятельными правовыми нормами, определяющими полномочия расследователей, порядок обращения с доказательствами и защиту прав вовлеченных лиц. В российском праве подобный закон отсутствует, что создает ситуацию, при которой границы допустимого определяются толкованием общих норм гражданского, трудового и уголовного законодательства. Для практической деятельности это означает необходимость постоянного юридического сопровождения: каждая операция по сбору и обработке информации должна оцениваться с точки зрения соответствия действующему законодательству.

Законодательство о персональных данных (152-ФЗ) устанавливает требования к обработке персональных данных, включая данные работников и контрагентов [31]. При проверке контрагентов экономическая разведка нередко обрабатывает персональные данные физических лиц: учредителей, руководителей, бенефициарных владельцев. Законность такой обработки определяется наличием правового основания: согласия субъекта данных, исполнения договора, обязанности оператора по законодательству или законного интереса оператора.

На практике установление правового основания может представлять значительную сложность, особенно при проверке лиц, не состоящих в договорных отношениях с компанией.

Уголовно-правовые ограничения затрагивают способы получения информации. Незаконное получение сведений, составляющих коммерческую тайну (статья 183 УК РФ), незаконное проникновение в компьютерную информацию (статья 272 УК РФ), нарушение тайны переписки (статья 138 УК РФ) образуют границы, за которыми заканчивается законная аналитическая деятельность и начинается преступление. Осознание этих границ является необходимым элементом профессиональной квалификации специалиста по экономической разведке. Экономическая разведка, как она понимается в настоящей работе, строится исключительно на законных источниках: открытых реестрах, публичной отчетности, судебных решениях, данных, полученных с согласия контрагентов, и сведениях из собственных информационных систем компании.

Вопрос о соотношении прав работодателя и прав работника при проведении внутренних проверок также требует рассмотрения. Трудовой кодекс Российской Федерации наделяет работодателя правом привлекать работников к дисциплинарной ответственности за нарушение трудовых обязанностей, однако порядок проведения служебных проверок и расследований регламентирован недостаточно четко. Практика корпоративных расследований в российских компаниях показывает, что основные правовые риски связаны с несоблюдением процедуры: проведением проверки без достаточных оснований, нарушением конфиденциальности результатов, использованием недопустимых методов сбора информации. Для минимизации этих рисков необходимы утвержденный локальный нормативный акт, определяющий основания, порядок и ограничения проведения внутренних проверок, а также юридическое сопровождение каждого случая.

Сравнительный анализ российских и зарубежных подходов к организации корпоративной разведки позволяет выделить несколько характерных различий. В американской практике due diligence (комплексная проверка) является стандартным элементом предынвестиционной оценки, сделок слияния и поглощения, крупных закупок и найма на руководящие должности. Процедура регулируется сочетанием федерального законодательства (Foreign Corrupt Practices Act, Dodd-Frank Act), отраслевых стандартов и судебной практики. В европейской традиции акцент смещен в сторону комплаенса и соблюдения регуляторных требований, особенно в области противодействия отмыванию доходов и коррупции. Директивы ЕС по борьбе с отмыванием денежных средств (Anti-Money Laundering Directives) обязывают финансовые организации проводить идентификацию клиентов и мониторинг транзакций, создавая спрос на профессиональные аналитические службы.

# Конец ознакомительного фрагмента.