

УДК 657.633.5

СУЩЕСТВЕННОСТЬ И РИСКИ ПРИ ПРОВЕДЕНИИ ВНУТРЕННЕГО КОНТРОЛЯ**Е.И. Ефремова, А.А. Филипенкова**

Российский экономический университет имени Г.В. Плеханова, Москва, email: es-audit@mail.ru, afilepenkova@internet.ru

Аннотация. Настоящая работа предлагает концепцию национального рекомендательного стандарта внутреннего контроля для частного коммерческого сектора России, призванную устранить существующий методологический вакуум. Концепция основана на адаптации международных практик (COSO IC/ERM, МОПП ПА) и предлагает трехуровневую модель: стратегический (группа компаний), уровень управления рисками (хозяйственные единицы) и операционный (подразделения). Стандарт детализирует методики оценки рисков и существенности для трёх ключевых областей: соблюдение законодательства, составление отчетности и операционная деятельность. Внедрение гибкого стандарта позволит компаниям создавать экономически обоснованные системы контроля, повышающие устойчивость и управляемость.

Ключевые слова: внутренний контроль, управление рисками, COSO ERM, COSO IC, три линии защиты.

MATERIALITY AND RISKS IN CONDUCTING INTERNAL CONTROL**E.I. Efremova, A.A. Filipenkova**

Russian Economic University named after G.V. Plekhanov, Moscow, email: es-audit@mail.ru, afilepenkova@internet.ru

Abstract. This work proposes a concept for a national recommended internal control standard for the private commercial sector in Russia, aimed at filling the existing methodological gap. The concept is based on the adaptation of international practices (COSO IC/ERM, IIA MOPP) and proposes a three-tier model: strategic (group of companies), risk management (business units), and operational (divisions). The standard details risk assessment and materiality methodologies for three key areas: compliance, reporting, and operations. The implementation of a flexible standard will allow companies to create cost-effective control systems that increase sustainability and manageability.

Keywords: internal control, risk management, COSO ERM, COSO IC, three lines of defense.

Дата поступления статьи в редакцию: 06.01.2026

Дата принятия статьи в печать: 27.02.2026

Введение

На данный момент не существует однозначного ответа на вопрос, какие методические нормативные акты должны использоваться внутренними контролерами при осуществлении внутреннего контроля на предприятии. Наиболее полно на национальном уровне в Российской Федерации представлены стандарты по внутреннему контролю банковских организаций и организаций государственного (муниципального) сектора (федеральные стандарты внутреннего государственного (муниципального) финансового контроля, они же ВГ(М)ФК, устанавливающие принципы и правила составления отчетности о результатах контрольной деятельности), но специальных стандартов по внутреннему контролю для частного коммерческого сектора не предусмотрено (за исключением некоторых ГОСТ Р ИСО, несущих рекомендательный характер).

При обращении к международным стандартам для внутреннего контроля, следует обратить внимание, что основу для определения существенности и рисков в практике внутреннего контроля составляют Международные стандарты внутреннего аудита (МСВА), которые с 9 января 2025 года заменили предыдущие МПСВА и являются центральной частью Международных основ профессиональной практики (МОПП/IPPF), разработанных Международным институтом внутренних аудиторов (IIA) и служащих с 1947 года универсальной основой для внутренних аудиторов по всему миру, для составления национальных законодательных актов и отраслевых рекомендаций. При этом важно разграничивать внутренний аудит (как независимую проверку) и внутренний контроль (как непрерывный процесс), хотя последний в своей методической работе может использовать как международные стандарты для внутреннего контроля, так и международные стандарты для внутреннего аудита, и также пользоваться национальными нормативными документами (например, ГОСТ) [6].

Объекты и методы исследования

В соответствии с указанными во введении рекомендательными стандартами первым этапом для внутреннего контролера является получение представления об объекте и оценка соответствующих рисков, что требует четкого определения самих понятий риска и существенности [10].

Риск определяется как «влияние неопределенности на достижение поставленных целей» (ГОСТ Р ИСО 31000-2019) [1]. Последствием реализации риска может быть как отклонение в негативную сторону, так и позитивная возможность, что важно учитывать в системе внутреннего контроля. Что касается существенности? Согласно рекомендациям, наиболее приближенным к существенности является понятие риск-аппетита (или толерантности риска) – той величины риска, которую организация готова принять для достижения своих целей.

Взаимосвязь этих понятий в системе внутреннего контроля проявляется в том, что существенность определяет порог, а риск характеризует вероятность и последствия его превышения. Эффективный внутренний контроль фокусирует ресурсы на областях, где риски превышают установленный уровень существенности.

В первую очередь для определения рисков и толерантности рисков, внутренний контролер должен быть обеспечен полной, достоверной и уместной информацией об объекте контроля.

Для формирования адекватного и всестороннего понимания объекта контроля перед внутренними аудиторами стоит задача сбора достоверной, релевантной и достаточной информации. Информационно-аналитическая база должна охватывать следующие ключевые аспекты:

1) стратегические ориентиры, целевые установки и профиль рисков организации, ассоциированных с аудируемым объектом;

2) установленный в организации допустимый уровень рисков (риск-аппетит) при его наличии;

3) результаты оценки рисков, послужившие основанием для формирования плана внутреннего аудита;

4) процессы руководства, риск-менеджмента и внутреннего контроля, действующие в рамках объекта проверки;

5) применимые концептуальные основы, руководящие принципы и иные критерии, позволяющие дать оценку эффективности указанных процессов [5].

При реализации консультационных заданий формальная документированная оценка рисков может не проводиться, если иное не оговорено с держателями акций, однако внутренние аудиторы обязаны выполнить ее базовый анализ для корректного понимания рискового ландшафта и определения ключевых фокус-областей.

На следующем этапе внутренние контролеры проводят аналитическую обработку собранных данных с целью моделирования должного функционирования исследуемых процессов. Идентификация рисков, подлежащих углубленному анализу, осуществляется через выявление потенциально существенных угроз достижению целей объекта контроля, учет специфических рисков мошенничества, а также оценку существенности и последующую приоритизацию выявленных рисков. Параллельно определяется система критериев, используемых руководством для оценки степени реализации контрольных целей. В случае, если профиль рисков по объекту уже был проанализирован в рамках предыдущих проверок, допускается актуализация существующей оценки. Исходной точкой для понимания объекта и оценки сопутствующих рисков является анализ обоснованности включения данного задания в план работы внутреннего контроля.

Методологический инструментарий для сбора необходимой информации включает:

1) анализ недавних оценок рисков, выполненных функцией внутреннего контроля, менеджментом или внешними провайдерами, с рассмотрением аспектов комплаенса, финансовой отчетности, операционной деятельности, мошенничества, информационных технологий и стратегии;

2) изучение информационных материалов по итогам ранее проведенных контрольных мероприятий, касающихся отчетности, соблюдения законодательства и операционной эффективности;

3) обращение к справочным материалам, таким как методические указания, стандарты (например, ГОСТ), руководства Международного института внутренних аудиторов, отраслевые и законодательные акты;

4) использование организационных схем и должностных инструкций для идентификации ответственных лиц;

5) учет установленных в организации категорий рисков (стратегические, операционные, финансовые, комплаенс) и анализ соответствующей документации – политик, процедур, отчетов, рабочих материалов прошлых проверок, а также данных о риск-аппетите.

Определение существенности рисков требует от внутренних контролеров применения профессиональных суждений, основанных на знаниях, опыте и критическом мышлении в отношении организации и целей задания. Проявляя должную профессиональную тщательность, аудиторам необходимо провести диалог с руководством объекта для согласования понимания бизнес-целей, ключевых рисков и терпимости к ним. Такой консенсус значительно повышает практическую ценность проводимой в рамках задания оценки рисков.

Обладая полной и достоверной информационной базой и принимая во внимание определение риска и толерантности риска, внутренний контролер обязан уметь рассчитывать риски и существенность внутри организации, которая является объектом его контроля. Для расчета и оценки внутренний контролер использует различную методологическую базу, указанную как в МОПП и ГОСТ, так и во внутренних документах организации.

Поделим методы определения рисков на три категории, в соответствии со сферами проверок внутреннего контроля:

- 1) на составление бухгалтерской отчетности,
- 2) соблюдения законодательства,
- 3) операционной деятельности. Каждая сфера требует своего расчета рисков и существенности (толерантности к риску), что будет рассмотрено далее [3].

Начать следует с определения рисков и существенности внутреннего контроля при составлении бухгалтерской отчетности. Существенность во внутреннем контроле (как и во внутреннем и во внешнем аудите в части, касающейся бухгалтерской отчетности) представляет собой пороговое значение (или качественный критерий), при превышении которого риск или отклонение считается неприемлемым и требует вмешательства контролей, а также внимания руководства.

Существует два основных метода расчёта существенности, который применяется при проведении внешнего аудита, но может использоваться в процессе осуществления внутреннего аудита и внутреннего контроля. Названия этих методов – дедуктивный и индуктивный [2].

Дедуктивный подход предполагает движение от общего к частному: сначала определяется общий уровень существенности для организации или отчетности в целом, который затем распределяется на отдельные элементы.

Пример расчета дедуктивным методом (табл. 1).

Таблица 1

Исходные данные из финансовой отчётности с необходимыми дополнениями для расчёта уровня существенности дедуктивным способом

| Базовые показатели | Значение, тыс. руб. | Доля, % | Применяемое значение, тыс. руб. |
|---------------------|---------------------|---------|---------------------------------|
| Балансовая прибыль | 21 289 | 5,0 | 1 064 |
| Выручка нетто | 135 968 | 2,0 | 2 719 |
| Валюта баланса | 128 138 | 2,0 | 2 563 |
| Собственный капитал | 20 500 | 10,0 | 2 050 |
| Общие затраты | 101 341 | 2,0 | 2 027 |

Источник: составлено авторами на основании [2].

Порядок расчётов следующий. Сначала мы рассчитываем среднее арифметическое: $(1\ 064 + 2\ 719 + 2\ 563 + 2\ 050 + 2\ 027)$ тыс. руб. / $5 = 2\ 085$ тыс. руб. Далее мы анализируем отклонения: наименьшее значение (1 064 тыс. руб.) отличается от среднего на 49,0%, наибольшее (2 719 тыс. руб.) – на 30,0%. На следующем шаге отбрасываем статистически значимые выбросы (1 064 тыс. руб.) и рассчитываем новое среднее: $(2\ 719 + 2\ 563 + 2\ 050 + 2\ 027)$ тыс. руб. / $4 = 2\ 335$ тыс. руб. Округляем до 2 500 тыс. руб. – получаем результат, единый уровень существенности. Этот общий уровень существенности затем распределяется между статьями баланса пропорционально их удельному весу.

Что касается индуктивного метода расчета существенности – индуктивный подход предполагает движение от частного к общему: сначала определяется существенность отдельных показателей, а затем их агрегирование для определения общего уровня существенности.

Пример расчет индуктивным методом представлен в таблице 2.

Таблица 2

Исходные данные из финансовой отчётности с необходимыми дополнениями для расчёта уровня существенности индуктивным способом

| Показатель | Значение, тыс. руб. | Уровень существенности, % | Уровень существенности, тыс. руб. (ст. 2 × ст. 3) |
|------------------------------|---------------------|---------------------------|--|
| Основные средства (А) | 207 | 5,0 | 10,35 |
| Запасы (А) | 420 | 2,0 | 8,40 |
| Дебиторы (А) | 380 | 2,0 | 7,60 |
| Уставный капитал (П) | 237 | 3,0 | 7,11 |
| Добавочный капитал (П) | 230 | 5,0 | 11,50 |
| Нераспределенная прибыль (П) | 140 | 10,0 | 14,00 |
| Займы (П) | 400 | 2,0 | 8,00 |

Источник: составлено авторами на основании [2].

Согласно таблице 2, при расчете индуктивным методом, сначала мы суммируем уровни существенности по статьям актива: $(10,35 + 8,40 + 7,60)$ тыс. руб. = 26,35 тыс. руб. (обычно тысячи рублей округляются строго для целей, но ради повышения точности расчетов при проведении операций округление будем производить до сотых). После этого суммируем уровни существенности по статьям пассива: $(7,11 + 11,50 + 14,00 + 8,00)$ тыс. руб. = 40,61 тыс. руб. Далее рассчитываем среднее арифметическое: $(26,35 + 40,61)$ тыс. руб. / 2 = 33,48 тыс. руб. Находим отношение к валюте баланса: $33,48 / 1007 \times 100,0\% = 3,3\%$.

Полученная величина в 33 тысячи рублей (округляем до целого значения) является единым показателем существенности для данной отчетности.

Следует выделить следующее сравнение методов и рекомендации по их применению (табл. 3).

Таблица 3

Сравнение двух методов расчёта существенности – индуктивного и дедуктивного [2]

| Критерий | Дедуктивный метод | Индуктивный метод |
|----------------|---|---|
| Направление | От общего к частному | От частного к общему |
| Фокус контроля | Проверка отчетности в целом на существенные искажения | Выявление качественно существенных искажений |
| Преимущества | Эффективное распределение ресурсов на значимые участки | Учет качественной существенности и эффекта совокупности мелких ошибок |
| Недостатки | Может не выявить искажения на малозначительных участках | Трудоемкость, требует выявления всех отклонений |

Источник: составлено авторами на основании [2].

На практике рекомендуется комбинировать оба подхода: использовать дедуктивный метод для определения общего уровня существенности и распределения аудиторских ресурсов, а индуктивный – для оценки эффекта совокупности искажений и выявления качественных нарушений.

От методики расчета существенности для бухгалтерской отчетности следует перейти к основным инструментам управления рисками в области соблюдения законодательства.

Процесс управления рисками соблюдения законодательства (комплаенс) начинается с определения границ оценки и формирования «регуляторной вселенной» – полного перечня применимых к компании законов, стандартов и внутренних политик, что реализуется через составление реестра рисков и картирование точек соприкосновения ключевых бизнес-процессов (например, заключение договоров, обработка данных, финансовые операции) с этими требованиями. На следующем этапе проводится анализ и оценка каждого выявленного риска путем присвоения баллов по вероятности его возникновения и потенциальному влиянию по финансовой, операционной, репутационной и юридической категориям, после чего рассчитывается интегральный «индекс риска» (вероятность × влияние) для их объективной приоритизации. Ключевым элементом является определение существенности, устанавливающей порог значимости риска или отклонения. Количественная (финансовая) существенность определяется как процент от ключевого финансового показателя (например, выручки), в то время как качественная существенность признает риск существенным вне зависимости от финансовой оценки – по своей при-

роде (подозрения в мошенничестве, коррупции, умышленном искажении) или по контексту (нарушения, вызывающие высокий интерес регуляторов или общественности), что в совокупности позволяет системе внутреннего контроля фокусировать ресурсы на наиболее значимых угрозах соблюдению законодательства.

Далее рассмотрим ключевые методики расчета рисков и аппетит-риска в сфере операционной деятельности – последнего, третьего элемента. Ключевыми методами расчета и управления риск в данном направлении являются матрица рисков или тепловая карта, модели «трех линий защиты» и модели COSO (классическая модель IC и расширенная модель ERM) [7].

Тепловая карта является такой методикой, которая при выполнении операционного задания приоритизирует по уровню существенности каждый из указанных в плане осуществления внутреннего контроля рисков. Расчет приоритизации зависит от каждого предприятия индивидуально; зачастую тепловая карта берет за основу для приоритизации вероятности реализации риска и тяжести его потенциальных последствий. Если риск в ходе анализа по тепловой карте оказывается существенным, то внутренние контролеры сперва определяют, какие именно контроли (превентивные, детективные, директивные или корректирующие) необходимо тестировать на операционную эффективность, на наличие узких мест или мест для улучшения и оптимизации ресурсов.

Схожей методикой является матрица рисков и контролей, но, в первую очередь, она создается не столько для приоритизации рисков, сколько для выявления структурных элементов конкретного риска, а именно – связанных с ним систем контроля, их типов, причин, последствий, а также оценки остаточных рисков по мере проведения тестирования, выполняя таким образом роль центрального инструмента визуализации и приоритизации, основанного на анализе вероятности и последствий рисков событий. [11].

Таблица 4

Матрица рисков на примере АО «РЖД»

| Вероятность / Влияние | Незначительное | Умеренное | Существенное |
|-----------------------|---------------------|-------------------------|-----------------------|
| Высокая | Риски поставок (S2) | Риски оборудования (S1) | Киберриски (S1) |
| Средняя | Риски ремонтов (S2) | Риски безопасности (S1) | Финансовые риски (S1) |
| Низкая | Кадровые риски (S3) | Риски отчетности (S2) | Риски соблюдения (S2) |

Источник: составлено авторами на основании [4].

S1 – риски, требующие немедленного вмешательства; S2 – риски, требующие контроля; S3 – риски, принимаемые к наблюдению. Для каждого риска, попадающего в зону «умеренное» и «существенное» влияние, разрабатываются контрольные процедуры, соответствующие установленному уровню существенности.

Модель «трех линий защиты», являясь ключевым элементом современной парадигмы внутреннего контроля (рекомендованной Международным институтом внутренних аудиторов), структурирует распределение ролей в организации, где первая линия (субъекты управления, такие как операционный менеджмент и владельцы процессов, как, например, руководители дирекций и филиалов в ОАО «РЖД») обеспечивает непосредственный контроль за рисками в повседневной деятельности; вторая линия (субъекты мониторинга, включающие специализированные подразделения – риск-менеджмент, комплаенс, безопасность, представленные в «РЖД» Департаментом управления рисками) отвечает за разработку методологии, мониторинг и координацию; а третья линия (субъекты независимой оценки, в лице внутреннего аудита, подчиняющегося в «РЖД» Совету директоров) проводит независимую оценку эффективности первых двух линий и системы внутреннего контроля в целом [4].

Что касается моделей COSO, то наиболее используемыми являются две указанные далее модели – модель COSO IC и модель COSO ERM. Первая модель является более традиционной и компактной и рассчитана больше как на текущий, так и на тактический уровень планирования и управления рисками во внутреннем контроле; в то время как COSO ERM является репрезентативной моделью для использования также и в стратегических целях.

Классическая модель COSO IC (The Committee of Sponsoring Organizations of the Treadway Commission, Internal Control) включает пять взаимосвязанных компонентов. В их число входят 1. Контрольная среда; 2. Оценка рисков; 3. Контрольные процедуры, 4. Информация и ком-

муникация, 5. Процедуры мониторинга. Все эти пять элементов распространяются как на всю организацию, так и на структурное подразделение, операционное подразделение и на конкретные функции внутри каждого из подразделений. При этом, когда речь заходит о внутреннем контроле, эти пять элементов рассматриваются с точки зрения трех элементов, таких как операционной деятельности, подготовки отчетности, комплаенса, то есть с точки зрения 1. операционных целей, 2. целей подготовки отчетности; 3. целей соблюдения законодательства [8].

Что касается дополненной модели COSO ERM (The Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management), то здесь появляется так называемая интегрированная модель управления рисками, которая состоит из восьми элементов, в том числе из:

- 1) внутренней среды,
- 2) постановки целей,
- 3) определения событий,
- 4) оценки рисков,
- 5) реагирования на риск,
- 6) средств контроля,
- 7) информации и коммуникации,
- 8) мониторинга.

Каждый из этих восьми элементов распространяется как и классическая модель на всю компанию, на подразделения и их функции; но также распространяется и в обратную сторону на увеличение масштаба – на дочерние организации, на сегменты группы, на всю группу компаний. Все эти элементы рассматриваются с четырех точек зрения: 1. стратегические цели, 2. операционные цели, 3. цели подготовки отчетности, 4. цели соблюдения законодательства. Можно заметить в сравнении с традиционной моделью, что расширенная модель ERM добавляет новую плоскость для рассмотрения деятельности объектов контроля – стратегическую, более долгосрочную и плановую область [9].

Разберемся в каждом элементе, сравним элементы расширенной модели с классической и приведем примеры того, какой вид приобретает каждый компонент на разных уровнях в предприятии.

1. Внутренняя среда (ERM) / Контрольная среда (IC).

С точки зрения всей компании Совет директоров утверждает политику управления рисками и этический кодекс, устанавливая «тон сверху», к примеру, через внедрение единых стандартов риск-культуры через:

1. Кодекс корпоративного управления;
2. Положение о единых требованиях к внутреннему контролю;
3. Регулярные оценки корпоративной культуры.

2. Постановка целей (ERM).

На стратегическом уровне постановка целей для всей организации может означать определение риск-аппетита и толерантности к рискам. Установление этого показателя начинается после определения контрольной среды, так как только после этого этапа компания может определить, какой показатель будет наиболее репрезентативно отражать эффективность ее деятельности. К примеру, организация в бизнес-сегменте может установить определенный процент прироста в своем сегменте реализации продукции – к примеру, увеличить поставку и экспорт нефти на 15,0% за отчетный год, увеличить продажу нефти в Российской Федерации на 7,0%, увеличить отпуск нефти на экспорт на 8,0% и пр., и дальше распространить постановку целей на каждое структурное подразделение, если был выбран способ «тона сверху».

3. Выявление событий (ERM).

С уровня всей организации мы спускаемся на уровень подразделений. Выявление событий может иметь как стратегический, так и оперативный характер. Чаще всего выявление событий служит нескольким уровням одновременно. Так, внутренний контроль головного тяжелого промышленного нефтеперерабатывающего предприятия может установить, что вводимые санкции на танкеры могут привести к тому, что поставки задержатся, либо вовсе не дойдут до организации. Внутренний контролер обеспечивает этой информацией структурные подразделения, которые затем выявляют, как это событие скажется на их деятельности. В случае с финансовым подразделением это будет означать, что снизится плановый финансовый поток; в случае с логистическим подразделением это будет означать, что будет необходим поиск новых танкеров или контрагентов, которые имеют более низкие риски попадания под санкции.

4. Оценка рисков (ERM) / Оценка рисков (IC).

На уровне хозяйственных подразделений с целью их объединения этот компонент предусматривает единый процесс идентификации рисков. Можно сказать, что примером данного компонента на уровне хозяйственных единиц может служить единый реестр рисков с классификацией по типам и уровням, который может создавать точные инструкции по выходу из критической ситуации при сбое оборудования; прописывание инструкции действий поведения работников по тому, как действовать во время поломок; частоту выведения из строя оборудования, а также негативные последствия таких событий, возможные финансовые потери для ремонта или замены сломанного оборудования.

5. Реагирование на риск (ERM) / Контрольные процедуры (IC).

На уровне структурных подразделений и функций подразделений контрольные процедуры и реагирование на риск предусматривает не столько действия работников при внештатных ситуациях и прописывание действий и поведения при критических событиях (как было описано в пункте 4), сколько попытка нивелирования риска одним из четырех возможных путей, описанных в научной литературе. Существует четыре типа реагирования на риск – избежание (на примере оборудование – отказ от покупки дешевых аналогов в ущерб качеству); принятие (покупка дешевого оборудования в тех сегментах, где ремонт стоит также дешево и может быть оперативно осуществлен на месте); снижение (введение дополнительных ремонтных станций в месте повышенного риска поломки оборудования); передача (страхование оборудование и аутсорсинг).

6. Средства контроля (ERM) / Информация и коммуникации (IC).

На уровне между подразделениями или межфункциональном уровне может обозначать систему отчетности и коммуникаций. Это могут быть ERP-система с модулями управления рисками и контроля; регулярные отчеты для руководства о состоянии ключевых контролей; система эскалации существенных отклонений; платформа для обмена информацией об инцидентах. Является одним из ключевых компонентов, который пронизывает все остальные компоненты. Без эффективной коммуникации и вовремя переданной информации все остальные компоненты могут терять свой смысл и иметь исключительно формальный и бюрократический смысл.

7. Мониторинг (ERM) / Процедуры мониторинга (IC).

Мониторинг должен быть неотъемлемой частью на всех уровнях (на уровне всей группы, сегментов, одной компании в группе, ее подразделений и функций подразделений) и осуществляться внутренним контролем на протяжении всего времени, включая периодические оценки и проверки. Такой мониторинг может подразделяться на виды – непрерывный, периодический, событийный. Непрерывный мониторинг может включать автоматический контроль соблюдения лимитов в ERP-системе; что касается периодического, то это может осуществляться в виде ежеквартальной оценки эффективности контролей внутренним аудитом; а событийный может включать в себя расследование инцидентов и специальные корректирующие действия для решения последствий инцидентов.

Заключение

Для устранения существующего методического вакуума в сфере внутреннего контроля частного коммерческого сектора настоятельно необходима разработка национального рекомендательного стандарта. Его создание должно стать результатом консенсуса между регуляторами, профессиональным сообществом и бизнесом, а методологическую основу следует формировать путем адаптации признанных международных подходов (таких как COSO ERM и МОПП) к национальным реалиям. Ключевой особенностью стандарта должно стать четкое структурирование требований по уровням организационной иерархии – от стратегического управления рисками на уровне группы компаний до оперативных контрольных процедур на уровне подразделений и их функций.

Стандарт должен предоставлять организациям детализированные, но гибкие методические рекомендации по оценке рисков и существенности в трех ключевых сферах: соблюдение законодательства (комплаенс), составление бухгалтерской отчетности и операционная деятельность. Для каждой сферы необходимо прописать соответствующие ей методы, такие как качественно-количественная оценка и картирование регуляторных требований для комплаенса, комбинация дедуктивного и индуктивного подходов для бухгалтерской отчетности, а также обязатель-

ное использование матриц, «трех линий защиты» и моделей компонентов механизма контроля для операционной деятельности.

Для обеспечения практической ценности стандарт должен закладывать принципы гибкой адаптации, а не жесткие догмы. К ним относится требование к организациям самостоятельно документировать выбранные методы и установленные пороги существенности, разрешение на комбинирование методик в зависимости от отраслевой специфики и масштаба, а также обязательство по непрерывному мониторингу и регулярному пересмотру системы контроля. Такой стандарт станет универсальной дорожной картой, позволяющей компаниям выстраивать экономически обоснованные и эффективные системы внутреннего контроля, соответствующие как национальным, так и международным ожиданиям.

Литература

1. Менеджмент риска. Принципы и руководство: ГОСТ Р ИСО 31000-2019 (IDT). Введ. 2020-09-01. [Электронный ресурс]. URL: <https://normativ.kontur.ru/document?moduleId=9&documentId=399742> (дата обращения: 14.11.2025).
2. Агаркова А.А., Калущая Н.А. Определение уровня существенности в аудите // Ответственный редактор. 2022. С. 5-7. EDN: PAQBZA.
3. Акимов А.С. Разработка системы управления рисками и внутреннего контроля // Финансовые рынки и банки. 2023. № 5. С. 5-9. EDN: EUCRNS.
4. Гапанович В.А., Шубинский И.Б., Проневич О.Б., Швед В.Э. Система управления рисками крупных компаний. Практика оценки рисков в ОАО «РЖД» и направления развития // Проблемы анализа риска. 2018. № 2. EDN: UPGHTC.
5. Передереева Е.В. Трансформация инструментария корпоративного финансового контроллинга в условиях цифровизации бизнес-процессов: дис. ... канд. экон. наук. Ставрополь, 2023. 221 с. EDN: WZIVJP.
6. Сабирова А.И., Тюленева Е.А. Особенности законодательных требований к внутреннему аудиту // Актуальные аспекты развития науки и общества в эпоху цифровой трансформации: сб. статей. Уфа, 2023. С. 166-171. DOI: 10.34755/IROK.2023.58.46.093. EDN: IPNBQM.
7. Швырева О.И., Роговская Н.И., Дюжева М.Б. Современные модели внутреннего контроля // Естественно-гуманитарные исследования. 2023. № 5(49). С. 310-317. EDN: HUDDWB.
8. Espinosa-Jaramillo M. T. Internal Control in Companies from the Perspective of the COSO // Management (Montevideo). 2024. Vol. 2. P. 28. DOI: 10.62486/agma202428. EDN: DXPVEU.
9. Shayb H.A. How COSO ERM and SHIMODEL algorithm can contribute to the development of enterprise performance // Journal of Social Sciences. 2021. Vol. 4, No. 2. P. 76-83.
10. Международные стандарты. Институт внутренних аудиторов. 2025. [Электронный ресурс]. URL: https://www.iaa-ru.ru/inner_auditor/professional/ (дата обращения: 14.11.2025).
11. Международные стандарты внутреннего аудита (МСВА): глобальная перспектива. 2023. [Электронный ресурс]. URL: <https://www.iaa-ru.ru/upload/inner-auditor/articles/2023-7726%20GUI%20Global%20IA%20Standards-Russian.pdf> (дата обращения: 14.11.2025).