Банк России

МАТЕРИАЛЫ ЗАСЕДАНИЯ ЭКСПЕРТНОГО СОВЕТА ПО РЕГУЛИРОВАНИЮ, МЕТОДОЛОГИИ ВНУТРЕННЕГО АУДИТА, ВНУТРЕННЕГО КОНТРОЛЯ И УПРАВЛЕНИЯ РИСКАМИ В БАНКЕ РОССИИ И ФИНАНСОВЫХ ОРГАНИЗАЦИЯХ ОТ 27 ФЕВРАЛЯ 2026 ГОДА

2026

СОДЕРЖАНИЕ

Редакционная коллегия дайджеста:

В.П. Горегляд, председатель редакционной коллегии, д.э.н.

М.А. Лауфер, к.э.н.

Н.А. Станик, к.э.н.

Материал подготовлен службой главного аудитора Банка России.

Ответственные за выпуск: Н.А. Станик, М.А. Лауфер.

Мнения, содержащиеся в материалах, являются личной позицией авторов и могут не совпадать с официальной позицией Банка России.

Комментарии, предложения и замечания можно направлять по адресу: expert.board@mail.cbr.ru.

107016, Москва, ул. Неглинная, 12, к. В

Официальный сайт Банка России: www.cbr.ru

ОБРАЩЕНИЕ ПРЕДСЕДАТЕЛЯ БАНКА РОССИИ К ЧИТАТЕЛЯМ

Уважаемые коллеги!

Современные системы контроля перестают быть исключительно инструментом выявления нарушений. Они становятся важным элементом стратегического управления, который позволяет выявлять новые угрозы, обеспечивать прозрачность процессов принятия решений и поддерживать устойчивость бизнеса в условиях высокой неопределенности и цифровой трансформации. И это касается всех отраслей без исключения.

Поэтому мы придаем большое значение деятельности нашего профильного Экспертного совета и стараемся привлекать к его работе представителей широкого круга компаний и академического сообщества. Рассчитываю, что предметное и профессиональное обсуждение самых злободневных вопросов и обмен лучшими практиками в конечном счете помогут нашему бизнесу устойчиво развиваться.

Э.С. Набиуллина
Председатель Банка России

ОБРАЩЕНИЕ ГЛАВНОГО АУДИТОРА БАНКА РОССИИ К ЧИТАТЕЛЯМ

Уважаемые коллеги!

Представляем вашему вниманию материалы заседания Экспертного совета по регулированию, методологии внутреннего аудита, внутреннего контроля и управления рисками в Банке России и финансовых организациях, состоявшегося 27 февраля 2026 года в Банке России в очно-дистанционном формате. Тема заседания – ***«Эволюция контрольной системы российских компаний в цифровую эпоху: комитет по аудиту как центр стратегической адаптации»*** *– отражает ключевые изменения, происходящие сегодня в сфере корпоративного управления, внутреннего аудита, внутреннего контроля и управления рисками.*

В работе заседания приняла участие Председатель Банка России Эльвира Сахипзадовна Набиуллина, что подчеркивает значимость обсуждаемой повестки для развития системы управления рисками и контрольной среды как в финансовом секторе, так и в российской экономике в целом. Совет продолжает выступать важной профессиональной площадкой, на которой формируется современная методология внутреннего аудита, внутреннего контроля и управления рисками. Его ключевая роль заключается не только в обсуждении актуальных вопросов, но и выработке практических решений и подходов, отвечающих текущим вызовам.

Особое внимание в ходе заседания было уделено трансформации контрольных систем в условиях цифровой экономики. Усложнение технологической среды, рост взаимосвязанности бизнес-процессов и расширение использования данных формируют новую конфигурацию рисков и предъявляют повышенные требования к эффективности контрольных систем. В этих условиях особое значение приобретает способность компаний выстраивать интегрированные системы управления рисками, внутреннего контроля и внутреннего аудита, способные обеспечивать устойчивость бизнеса и поддерживать реализацию стратегических целей.

В центре обсуждения на заседании находились вопросы развития стратегического аудита как инструмента обеспечения устойчивости компаний в период цифровой трансформации, эволюции роли комитетов по аудиту в системе корпоративного управления, а также формирования новых компетенций специалистов внутреннего аудита в условиях цифровизации.

В представленных материалах рассматриваются практические подходы к развитию функций внутреннего аудита, внутреннего контроля и управления рисками, включая вопросы построения интегрированных контрольных систем в технологических компаниях, развития цифровых компетенций сотрудников

внутреннего аудита и применения современных технологических решений для повышения эффективности контрольной среды.

Отдельное внимание уделено новым объектам аудита и контроля, возникающим в условиях цифровизации бизнес-процессов, а также управлению технологическими рисками, включая риски информационных технологий, киберриски и риски, связанные с использованием искусственного интеллекта.

Материалы заседания отражают как методологические подходы, так и практический опыт российских компаний финансового и реального сектора. Представленные исследования и кейсы демонстрируют, что функции внутреннего аудита, внутреннего контроля и управления рисками все в большей степени становятся элементами стратегического управления и важным фактором обеспечения устойчивости компаний в условиях высокой неопределенности и технологических изменений.

Надеемся, что представленные материалы будут полезны специалистам в области внутреннего аудита, внутреннего контроля и управления рисками, членам советов директоров и комитетов по аудиту, руководителям организаций, а также всем, кто заинтересован в развитии эффективных систем корпоративного управления.

В.П. Горегляд
Главный аудитор Банка России, председатель Экспертного совета по регулированию, методологии внутреннего аудита, внутреннего контроля и управления рисками в Банке России и финансовых организациях

ВСТУПЛЕНИЕ

Настоящий выпуск подготовлен по итогам заседания Экспертного совета по регулированию, методологии внутреннего аудита, внутреннего контроля и управления рисками в Банке России и финансовых организациях, состоявшегося **27 февраля 2026 года в Банке России**.

Современные организации функционируют в условиях возрастающей технологической сложности и высокой неопределенности внешней среды. Расширение использования цифровых технологий, рост зависимости бизнес-процессов от информационных систем и данных, а также развитие технологий искусственного интеллекта формируют новую конфигурацию рисков. В этих условиях особое значение приобретает способность организаций своевременно выявлять угрозы, адаптироваться к изменениям и поддерживать устойчивость своих бизнес-моделей.

Важную роль в обеспечении устойчивости организаций играют эффективные системы внутреннего контроля, внутреннего аудита и управления рисками. Современные контрольные системы становятся важным элементом стратегического управления, обеспечивая независимую оценку эффективности управленческих решений и поддерживая реализацию стратегических целей организаций.

Материалы настоящего выпуска объединяют исследования и практические кейсы экспертов в области внутреннего аудита, внутреннего контроля и управления рисками. Представленные статьи отражают различные аспекты трансформации контрольных систем и демонстрируют практические подходы к развитию функций внутреннего аудита и управления рисками в условиях цифровой экономики.

Благодарность авторам

Редакционная коллегия дайджеста выражает искреннюю благодарность авторам статей за представленные материалы и активное участие в профессиональной дискуссии, посвященной вопросам развития внутреннего аудита, внутреннего контроля и управления рисками.

Подготовленные авторами исследования и аналитические материалы отражают как методологические подходы, так и практический опыт российских организаций и финансовых институтов. Представленные в сборнике публикации способствуют развитию профессионального диалога и формированию современных подходов к организации эффективных систем внутреннего контроля и управления рисками.

Редакция также благодарит участников заседания совета за конструктивное обсуждение актуальных вопросов развития контрольных систем и обмен практическим опытом.

Итоги заседания совета

Центральной темой заседания стала **эволюция контрольной системы российских компаний и новая роль комитетов по аудиту как центров стратегической адаптации организаций**.

В ходе заседания была проведена содержательная профессиональная дискуссия, охватившая ключевые направления развития современных систем контроля и управления рисками.

ТРАНСФОРМАЦИЯ РОЛИ ВНУТРЕННЕГО АУДИТА В ЦИФРОВОЙ ЭКОНОМИКЕ

Одним из центральных выводов заседания стало признание того, что **функция внутреннего аудита претерпевает фундаментальные изменения**.

Если ранее внутренний аудит в основном рассматривался как инструмент выявления нарушений и контроля соблюдения процедур, то в условиях цифровой трансформации его роль существенно расширяется.

Сегодня внутренний аудит становится:
- инструментом **оценки устойчивости стратегий организаций**;
- элементом **системы стратегического управления рисками**;
- механизмом **независимой оценки эффективности корпоративного управления**;
- ключевым **источником информации** для советов директоров и комитетов по аудиту.

Особое внимание участники заседания уделили концепции **стратегического аудита**, который позволяет оценивать не только корректность стратегических решений, но и способность компании реализовать выбранную стратегию в условиях высокой неопределенности и технологических изменений.

КОМИТЕТ ПО АУДИТУ КАК ЦЕНТР СТРАТЕГИЧЕСКОЙ АДАПТАЦИИ

Значительная часть обсуждения была посвящена **эволюции роли комитетов по аудиту советов директоров**.

Отмечалось, что в современной корпоративной практике комитет по аудиту выходит далеко за рамки традиционной функции контроля финансовой отчетности.

Комитет по аудиту становится:
- ключевым элементом **инфраструктуры доверия на рынке капитала**;
- площадкой для **интеграции стратегических, технологических и риск-управленческих решений**;
- органом, обеспечивающим **независимый надзор за системой внутреннего контроля и управления рисками**;
- механизмом обеспечения **прозрачности управленческих решений и устойчивости бизнеса**.

Особое внимание было уделено международной практике развития комитетов по аудиту, включая опыт США, стран Европейского союза и азиатских рынков, где усиление роли комитетов стало ответом на корпоративные скандалы и финансовые кризисы последних десятилетий.

Участники дискуссии отметили, что дальнейшее развитие комитетов по аудиту в российских компаниях должно сопровождаться:
- усилением независимости членов комитетов;
- повышением профессиональной компетенции независимых директоров;
- расширением взаимодействия комитетов с внутренним и внешним аудитом;
- активным использованием цифровых инструментов анализа и мониторинга рисков.

ЦИФРОВИЗАЦИЯ КАК НОВЫЙ ИСТОЧНИК РИСКОВ

Отдельное внимание было уделено **изменению структуры рисков в условиях цифровой трансформации экономики**.

Участники заседания подчеркнули, что развитие цифровых технологий приводит к возникновению новых категорий рисков, включая:
- технологические риски;
- киберриски;

- риски, связанные с качеством и управлением данными;
- риски использования алгоритмов и систем искусственного интеллекта;
- риски зависимости организаций от цифровых платформ и внешних технологических поставщиков.

В этой связи современные системы внутреннего контроля должны учитывать не только традиционные финансовые и операционные риски, но и **риски цифровой инфраструктуры компаний**.

Было отмечено, что для эффективного управления такими рисками необходимо развитие интегрированных систем управления, объединяющих:
- управление рисками;
- внутренний контроль;
- внутренний аудит;
- управление данными;
- технологическое управление.

НОВЫЕ КОМПЕТЕНЦИИ СПЕЦИАЛИСТОВ ВНУТРЕННЕГО АУДИТА

Участники заседания уделили значительное внимание вопросам **развития профессиональных компетенций специалистов внутреннего аудита**.

Было отмечено, что традиционные навыки аудиторов должны дополняться новыми знаниями и компетенциями, включая:
- анализ больших данных;
- аудит информационных систем;
- понимание архитектуры цифровых платформ;
- оценку алгоритмических моделей и систем искусственного интеллекта;
- использование современных аналитических инструментов.

Особый интерес участников вызвал опыт российских компаний по формированию цифровых компетенций сотрудников внутреннего аудита, включая использование систем управления знаниями и интеллектуальных ассистентов на основе технологий генеративного искусственного интеллекта.

ИНТЕГРАЦИЯ СИСТЕМ ВНУТРЕННЕГО КОНТРОЛЯ, АУДИТА И УПРАВЛЕНИЯ РИСКАМИ

Важным выводом стала необходимость **перехода к интегрированным контрольным системам**.

Участники заседания отметили, что в современных организациях функции внутреннего контроля, внутреннего аудита и управления рисками должны рассматриваться не как отдельные элементы корпоративной структуры, а как **единая система обеспечения устойчивости бизнеса**.

Такая система должна обеспечивать:
- своевременное выявление угроз;
- поддержку принятия управленческих решений;
- контроль реализации стратегических инициатив;
- повышение прозрачности процессов управления.

ПРАКТИЧЕСКИЕ КЕЙСЫ ТРАНСФОРМАЦИИ КОНТРОЛЬНЫХ СИСТЕМ

В рамках заседания были представлены практические кейсы российских организаций, демонстрирующие различные подходы к трансформации контрольных систем.

В частности, были рассмотрены:
- применение стратегического аудита в крупных инфраструктурных компаниях;
- цифровая трансформация функций внутреннего аудита;
- автоматизация процессов управления рисками и внутреннего контроля;
- развитие технологий обучения и передачи знаний в службах внутреннего аудита.

Представленные кейсы показали, что современные компании активно внедряют новые подходы к управлению рисками и контролю, ориентированные на использование цифровых технологий и аналитики данных.

ЗНАЧЕНИЕ ЭКСПЕРТНОГО СОВЕТА КАК ПРОФЕССИОНАЛЬНОЙ ПЛОЩАДКИ

По итогам заседания участники отметили важную роль Экспертного совета как **уникальной профессиональной платформы для диалога между регулятором, бизнесом и академическим сообществом**.

Совет выполняет несколько ключевых функций:
- формирование методологических подходов к развитию систем внутреннего контроля и аудита;
- обмен практическим опытом между финансовыми организациями и компаниями реального сектора;
- обсуждение международных практик корпоративного управления;
- развитие профессионального сообщества специалистов по внутреннему аудиту и управлению рисками.

Заседание Экспертного совета подтвердило, что в условиях цифровой трансформации экономики системы внутреннего контроля, внутреннего аудита и управления рисками становятся важнейшими элементами устойчивого развития организаций.

Современные контрольные системы должны быть ориентированы не только на выявление нарушений, но и на:
- поддержку стратегического управления;
- повышение прозрачности и доверия на рынке капитала;
- обеспечение технологической и операционной устойчивости компаний.

Развитие этих систем требует активного взаимодействия регуляторов, бизнеса и профессионального сообщества, внедрения современных цифровых технологий и формирования новых компетенций специалистов в области аудита и управления рисками.

Материалы настоящего сборника отражают результаты профессиональной дискуссии и представляют практический вклад в развитие современных подходов к корпоративному управлению, внутреннему аудиту и управлению рисками в российской экономике.

СТРАТЕГИЧЕСКИЙ АУДИТ КАК ИНСТРУМЕНТ УСТОЙЧИВОГО РАЗВИТИЯ КОМПАНИИ В ПЕРИОД ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Стратегический аудит сегодня перестает быть проверкой стратегии как документа. Он становится инструментом оценки устойчивости управленческой системы компании в условиях цифровой трансформации и высокой неопределенности.

А.И. АРХАНГЕЛЬСКАЯ
Группа «Московская Биржа», независимый директор

Аннотация

Цифровая трансформация радикально меняет характер стратегических рисков: к рыночной и операционной волатильности добавляются архитектурные ограничения ИТ-ландшафта, качество данных, киберугрозы и зависимость от экосистем поставщиков. В этих условиях стратегический аудит перестает быть разовой «проверкой стратегии как документа» и превращается в системный механизм уверенности для совета директоров: он увязывает стратегические цели, риск-аппетит, портфель инициатив, организационную архитектуру и цифровую устойчивость. В статье предложен практический подход к стратегическому аудиту на основе новых IIA Global Internal Audit Standards (2024) (далее – IIA 2024) и сопряженных международно признанных стандартов (COSO ERM, ISO 31000, ISO 37000, COBIT 2019, NIST CSF 2.0, ISO/IEC 27001), а также обоснована роль комитета по аудиту как «центра стратегической адаптации» и гаранта устойчивости трансформаций. Приведены наблюдения из российской и международной практики.

Ключевые слова: стратегический аудит; цифровая трансформация; корпоративное управление; риск-менеджмент; киберустойчивость; внутренний аудит; комитет по аудиту.

Коды JEL: M48, G34, O32, M15, D81.

Введение

Последнее десятилетие стало временем ускоряющегося «сдвига платформ» в корпоративном управлении: цифровизация бизнеса, рост зависимости от внешних провайдеров и данных, распространение облачных платформ, ИИ-решений и открытых экосистем коренным образом изменили профиль стратегических рисков. Традиционная оптика – когда «стратегия» мыслилась как тщательно отредактированный документ с наборами целей и KPI[1] – перестала работать. Реальная ценность и уязвимость стратегии сегодня определяются не красотой формулировок, а управляемостью сложной системы: качеством гипотез и допущений, дисциплиной перераспределения ресурсов, архитектурной целостностью ИТ-ландшафта, скоростью корректировок по «слабым сигналам», устойчивостью к киберрискам и зрелостью культуры исполнения.

[1] KPI – ключевые показатели эффективности.

На этом фоне стратегический аудит перестал быть разовой проверкой «логики стратегии» или формальной сверкой документов. Он превращается в механизм независимой уверенности для совета директоров: связывает стратегические цели, риск-аппетит, портфель инициатив, ресурсы, организационные роли, цифровые платформы и поведение людей в целостный контур. По сути, речь идет о сшивке управления, рисков, технологий, данных и культуры – причем в динамике, в моменте принятия решений, а не постфактум. Такой аудит живет в годовом плане службы внутреннего аудита (СВА), опирается на обновленные стандарты (IIA 2024; COSO ERM; ISO 37000; ISO 31000; COBIT 2019; NIST CSF 2.0; ISO/IEC 27001; при необходимости – BCBS 239[2]) и адресует не только вопрос «что замыслено?», но и «как это будет стабильно работать в условиях неопределенности?».

Ключевой вызов для управленцев в том, что устойчивость трансформации – это не сумма лучших практик по функциям, а способность компании быстро находить и устранять системные узкие места: дисбаланс между амбициями и ресурсами, хрупкость архитектуры, «технический долг», дублирующиеся и противоречивые метрики, зависимость от третьих сторон без надлежащих контуров контроля, неопределенность риск-аппетита, стимулы, провоцирующие искажающее поведение. Именно здесь стратегический аудит становится инструментом управляемости и обратной связи для совета и менеджмента крупных компаний.

Как изменился стратегический аудит: от «документа» к интеграции с управленческой системой

Исторически глубина и качество стратегического аудита были крайне неоднородными. Часто аудит опирался на внешние методологии (7-S McKinsey, BSC Kaplan & Norton и другие) и ограничивался составлением чек-листа корректности стратегии как документа и базовых связок с KPI/OKR[3]. В таком подходе фактическая реализация – процессы принятия решений, распределение ресурсов, устойчивость портфеля инициатив, качество данных, киберуправление – часто оставалась в тени. Цифровая трансформация сделала эту слепую зону критической.

Современный подход кардинально иной. Во-первых, акцент смещается на внутренний аудит как на третью линию защиты, формирующую независимую уверенность по стратегическим рискам и трансформационным программам. Это не «аудит стратегии» в узком смысле, а системная проверка управляемости: от качества допущений и сценариев до дисциплины go/kill/hold/pivot[4] по инициативам, от риск-аппетита до интеграции с операционными и иными рисками, от ресурсной модели до стимулов и организационной культуры. Во-вторых, аудит осмысляется как непрерывный процесс, встроенный в управленческий цикл и поддерживаемый панелями мониторинга (дашбордами) стратегических рисков и метрик зрелости. В-третьих, в повестку органично включается цифровая устойчивость: кибербезопасность, агрегируемость и качество управленческих данных, архитектурная целостность, управление жизненным циклом моделей (AI/ML/GenAI[5]).

Эволюцию институционализируют и стандарты. IIA 2024 усиливают требования к стратегическому планированию и непрерывному совершенствованию функции внутреннего аудита, вводят тематические требования (Topical Requirements), среди которых – кибербезопасность (выпуск 2025 года, вступление в силу 05.02.2026). В совокупности с COSO ERM (интеграция риск-менеджмента со стратегией и результативностью), ISO 37000 (надлежащее

---

2 Полные наименования по всем стандартам см. в списке литературы.

3 OKR (Objectives & Key Results) – цели и ключевые результаты.

4 «К реализации / закрыть / приостановить / изменить траекторию».

5 ИИ, машинное обучение, генеративный ИИ.

управление и подотчетность совета), ISO 31000/ГОСТ Р (принципы риск-менеджмента), COBIT 2019 (управление цифровыми активами), NIST CSF 2.0 (с функцией Govern, выводящей киберриски на уровень стратегии), ISO/IEC 27001 (Система менеджмента информационной безопасности, СМИБ) и для банков – BCBS 239 (агрегация данных о рисках) получается комбинация, которая позволяет аудиторам проверять не только «что написано», но и «как это работает как система».

Почему стратегический аудит критичен в эпоху цифровой трансформации

Цифровая трансформация изменяет не только технологии, но и экономику принятия решений. Внешняя среда приносит высокую регуляторную волатильность, эффект сети (network effects), конкуренцию экосистем и платформ, новые формы концентрации рисков на узловых поставщиках. Внутри компании растет сложность ИТ-ландшафта: микросервисы соседствуют с монолитами, бизнес-критичные процессы зависят от облачных сервисов, «технический долг» тормозит скорость изменений, а данные живут в разрозненных доменах. Любая из этих слабых точек может стать узким горлышком всей стратегии.

Поэтому стратегический аудит включает оценку цифровой устойчивости как необходимого условия жизнеспособности стратегии. На практике это означает: проверку зрелости киберуправления (включая роли совета и топ-менеджмента), построение профиля по NIST CSF 2.0 (особенно по функции Govern), согласование ИТ-портфеля со стратегическими целями и риск-аппетитом, управление архитектурной целостностью и «техническим долгом», контроль качества данных и прозрачной управленческой отчетности («одна версия правды»), а также зрелое управление жизненным циклом моделей (целевое назначение, ограничения, источники данных, этика и предвзятость (bias), объяснимость, валидация/ревалидация, матрица ответственности RACI по трем линиям). Все это не дополнительные опции, а ядро управления рисками реализации стратегии.

Важно понимать: в трансформации скорость обратной связи и способность перегруппировывать ресурсы решают больше, чем совершенство исходного плана. Там, где стратегический аудит встроен в управленческий цикл как «локатор хрупкости», компания увеличивает шансы на адаптивную устойчивость: вовремя видит провалы допущений, аудиторские сигналы превращаются в корректирующие действия, а комитет по аудиту получает объективную картину остаточного риска в привязке к целям.

Роль комитета по аудиту: лидерство и гарантия устойчивости

В новых условиях комитет по аудиту выходит за пределы традиционной финансовой повестки и становится местом, где сходятся стратегия, риски, технологии и культура исполнения. Его лидерство проявляется в нескольких плоскостях.

1. *Формирование повестки независимой уверенности*. Комитет утверждает риск-ориентированный план СВА, задает покрытие стратегических рисков и требует от внутреннего аудита собственной стратегии (требование IIA 2024), согласованной с целями компании. Это позволяет перейти от «проверок по факту» к системной, направленной в будущее уверенности по ключевым трансформационным темам.
2. *Комбинированная уверенность и карта гарантий*. Комитет координирует карту гарантий по каждой стратегической цели / риску: кто «владелец уверенности» – 1, 2 или 3-я линия, где нужны внешние провайдеры, каков уровень остаточного риска сейчас и в динамике. Такая конструкция предотвращает слепые зоны и дублирование усилий, экономит ресурсы и повышает прозрачность.

3. *Институционализация цифровой повестки*. Комитет вводит кибер- и операционную устойчивость в регулярную повестку, требует профилирования по NIST CSF 2.0 и COBIT 2019, задает требования к управлению модельными рисками (включая AI/ML/GenAI), качеству данных, управлению третьими сторонами и облаками. Это конвертирует технические вопросы в управленческие решения о приоритетах и ресурсах.
4. *Переход от отчетности к управлению*. Комитет вводит KPI стратегического аудита (доля охвата стратегических рисков в плане; процент инициатив с подтвержденной связностью «цель – риск – контроль – метрика»; сокращение «технического долга» в критических системах и другие) и дашборд стратегических рисков, совмещающий уровни риска по ключевым направлениям/проектам с метриками зрелости по COBIT и NIST CSF 2.0. Отчетные таблицы превращаются в дашборды.

В результате комитет по аудиту становится центром «стратегической адаптации» – органом, который надзирает не только за фактическими рисками, но и за скоростью обучения компании, контролируя удержание риск-профиля в допустимых границах и фокус ресурсов на действительно стратегических узких местах.

Что именно проверяет стратегический аудит: программа и объекты

Практическая программа стратегического аудита строится вокруг нескольких взаимосвязанных блоков:

1. *Качество стратегии и допущений*. Проверяется корректность стратегического анализа, гипотез и сценариев; наличие «петли» проверки гипотез (в духе замкнутого цикла управления по Kaplan & Norton). Цель – убедиться, что стратегия живет вместе с реальностью, а не застывает в документе.
2. *Каскадирование и измеримость*. Аудит изучает карту стратегии / сбалансированную систему показателей (ССП)[6], причинно-следственные связи, KPI/OKR, механизмы отслеживания (контроля) достижения выгод (эффектов), частоту стратегических ревью. Важно, чтобы метрики действительно отражали причинность, а не являлись набором «желательных чисел».
3. *Риск-аппетит и интеграция с COSO ERM*. Оценивается покрытие стратегических рисков, наличие критериев/метрик риска, связность с иными рисками. Без ясного риск-аппетита стратегическая амбиция часто превращается в гонку за метриками без учета волатильности.
4. *Портфель стратегических инициатив*. Анализируются правила отбора, этапные решения (go/kill/hold/pivot), инвестиционная дисциплина, способность останавливать «не те» проекты и перераспределять ресурсы. Это ключ к снятию узких мест и борьбе с эффектом утопленных затрат.
5. *Ресурсообеспеченность*. Проверяется приоритизация бюджета и капитала; соответствуют ли связки «люди – компетенции – данные – ИТ-мощности» стратегическим приоритетам; выявляются критические способности и узкие места.
6. *Контуры непрерывного улучшения*. Убедиться, что циклы «план – исполнение – ревью – коррекция» действительно работают на уровне стратегии, а не только в операционном контуре.
7. *Стимулы и вознаграждение*. Проверяется, не провоцируют ли KPI/бонусы искажающее поведение; соответствуют ли стимулы целям и риск-аппетиту.
8. *Организационная модель и культура*. Оценивается согласованность операционной модели, «тон сверху», роли и ответственность совета/комитетов; адекватно ли распределена ответственность за трансформацию, нет ли размывания критических ролей.

---

[6] Balanced Scorecard, BSC.

9. *Устойчивость и непрерывность*. Как цели и программы учитывают долгосрочную устойчивость (операционную и киберустойчивость), готовность к кризисным сценариям и регуляторным изменениям.
10. *Третьи стороны и экосистема*. Управление подрядчиками, альянсами, облачными провайдерами; учет новых тематических требований IIA 2024 по третьим сторонам; матрицы управления риском в экосистеме.
11. *Данные и управленческая отчетность*. Качество мастер-данных, реестр критичных показателей и источников, механизмы контроля целевых допусков, связка с политикой управления данными и СМИБ. Это фундамент «одной версии правды».
12. *Архитектурная целостность и «технический долг»*. Степень зависимости от устаревших систем, концентрация рисков на монолитах, жизненный цикл платформ/данных, планы миграции, критерии definition of done для снятия ограничений.
13. *Управление жизненным циклом моделей (AI/ML/GenAI)*. Четкость целевого назначения, допусков/ограничений, контроль источников данных, оценка предвзятости (bias) / этики, объяснимости, валидация/ревалидация, мониторинг дрейфа, распределение ролей по 1, 2 или 3-й линии.

Выходные артефакты – это инструменты дальнейшего управления: рекомендации по стратегическому циклу, тепловая карта стратегических инициатив, реестр критичных OKR/KPI/KRI[7], профили по NIST CSF 2.0 и COBIT 2019, оценка зрелости управления моделями, матрицы по третьим сторонам и экосистемам.

Интеграция стандартов: практическая «сборка»

Сила современного стратегического аудита – в согласованном применении нескольких стандартов, каждый из которых отвечает за свою плоскость управляемости (приведены, как пример, международно признанные стандарты):

1) IIA 2024 – «рамка» для самой функции СВА: стратегия функции, независимость, планирование, цикл улучшения, тематические требования. Это «метастандарт» для того, как аудит должен быть устроен и что он обязан покрывать;
2) COSO ERM – мост между стратегией и рисками: определение риск-аппетита, интеграция рисков в постановку целей и в performance-контур, процедуры пересмотра и корректировки;
3) ISO 37000 – «надлежащая управляемость»: роли, ответственность и подотчетность совета и комитетов; поведенческое измерение управления;
4) ISO 31000/ГОСТ Р – принципы и процесс риск-менеджмента на уровне всей компании, обеспечивающие единую терминологию и «скелет» практик;
5) COBIT 2019 – управление цифровыми активами и производительностью; понимание того, как в целом построено управление технологиями в компании: цели управления, практики, показатели зрелости;
6) NIST CSF 2.0 – профиль киберустойчивости с новой функцией Govern, которая поднимает кибербезопасность с уровня технологической дисциплины на уровень рисков компании в целом и стратегических решений;
7) ISO/IEC 27001 – базовые требования к СМИБ;
8) BCBS 239 – для банков: принципы агрегируемости данных о рисках и качественной риск-отчетности, применимые к стратегическим рискам и агрегации.

Комбинация этих стандартов – рабочая архитектура проверки, максимально полно покрывающая современные факторы стратегического риска. Например: COSO ERM отвечает на вопрос «каков риск-аппетит и как он интегрирован в цели и исполнение», COBIT – «насколько зрелы

[7] Key Risk Indicator – ключевой показатель риска.

механизмы управления ИТ и данными», NIST CSF – «как выглядят профили киберустойчивости и зоны повышенного остаточного риска», IIA 2024 – «достаточен ли по масштабу и качеству сам контур независимой уверенности». Вместе они дают аудитору сквозную линию доказательств – от допущений до данных и решений.

Кейсы и практические уроки

Опыт передовых организаций иллюстрирует, как стратегический аудит помогает управлять устойчивостью.

ГК «Росатом» (2023-2024). Фокус – реалистичность и исполнимость целей, качество ранних сигналов внешней среды, управление стратегическими рисками, согласованность метрик с ресурсной моделью и портфелем проектов. Это аудит жизнеспособности стратегии на длинном горизонте и скорости управленческих реакций. Урок: стратегический аудит при продуманном подходе и правильном использовании его результатов менеджментом компании можно превратить во встроенный в контур управления радар: он оценивает релевантность и реализуемость целей на длинном горизонте, настраивает систему ранних сигналов и триггеров и превращает риски в своевременные управленческие решения.

UNICEF India (2018-2021). В фокусе – выравнивание страновой программы с глобальной стратегией, архитектура партнерств и подотчетность как основа легитимности и устойчивости результатов; гибкость аудита (в том числе удаленный формат в пандемию) лишь подчеркнула важность управляемости сложной экосистемы. Урок: стратегический аудит – о связности целей, ресурсов и партнерств.

Еврокомиссия (2018-2019). Горизонтальные performance-аудиты по сквозным механизмам (непрерывность бизнеса, synergies & efficiencies, экосистема Horizon 2020) – вклад в performance-based culture и доставку приоритетов. Урок: аудировать нужно не только «вертикали», но и горизонтальные системы, которые обеспечивают скорость и качество исполнения стратегических инициатив.

Группа «Московская Биржа» (2025-2026). Новая стратегия внутреннего аудита до 2028 года включает оценку вклада/влияния на выполнение стратегических целей в каждую проверку, проводимую СВА, такая оценка шаблонизирована, регулярные проверки стратегических инноваций и «горизонтальных платформ» включены в аудиторский цикл на регулярной основе. Урок: системность аудита, фокус на влиянии на стратегию и оценка управляемости инноваций повышают долгосрочную устойчивость системно значимой инфраструктуры финансового рынка.

Организация процесса: дорожная карта для СВА и комитета по аудиту

Чтобы стратегический аудит работал как механизм адаптации, а не как набор разрозненных проверок, полезно выстроить следующую дорожную карту.

Шаг 1. Уточнить мандат и роли.

Комитет по аудиту обновляет мандат исходя из цифровой повестки (киберуправление, данные, модели, третьи стороны), утверждает стратегию функции СВА (IIA 2024), определяет набор стратегических рисков и критерии материальности для отбора объектов стратегического аудита, усиливает мандат СВА по стратегической повестке.

Шаг 2. Сформировать карту гарантий по стратегическим рискам.

На каждую стратегическую цель и риск фиксируется, кто отвечает за уверенность, какие источники подтверждения используются (1, 2 или 3-я линия, внешние провайдеры), какие пробелы покрываются стратегическим аудитом. Это снижает дублирование и закрывает слепые зоны.

Шаг 3. Встроить цифровую устойчивость в план работы комитета по аудиту.

На контроль ставятся профили по NIST CSF 2.0 и COBIT 2019 и критические зависимости (облака, вендоры, данные, модели), намечаются области для целевых проверок (архитектурная целостность, качество данных, MRM/AI-governance[8], непрерывность, кризисные сценарии), результаты выносятся на «стратегическую панель мониторинга» комитета.

Шаг 4. Настроить стратегический фокус в аудиторском цикле и регулярной повестке комитета по аудиту.

Элементы стратегического аудита интегрируются в другие проверки в качество элемента оценки достижения стратегических целей или стратегической устойчивости. Комитет может сформировать «стратегическую панель мониторинга», а также отслеживать специально установленные метрики полноты выполнения стратегического аудита или его элементов в аудиторском цикле.

Заключение

Стратегический аудит сегодня – это не про содержание стратегического документа, а про управляемость стратегии в реальном времени: насколько цели, риски, технологии, данные, архитектура, ресурсы и культура действительно увязаны так, чтобы компания достигала результатов при допустимом риск-профиле. Цифровая трансформация делает эту проверку критичной, потому что любая хрупкость – в данных, моделях, архитектуре, зависимостях от третьих сторон, киберконтуре или системе стимулов – мгновенно масштабируется и влияет на устойчивость бизнеса.

Именно комитет по аудиту обладает мандатом и инструментами, чтобы превратить стратегический аудит в «двигатель адаптации»: задать повестку независимой уверенности, институционализировать цифровую устойчивость, обеспечить комбинированную уверенность и перевести отчетность в управленческие решения через KPI и дашборды. Там, где этот механизм отстроен, совет управляет устойчивостью не постфактум, а в моменте – и тем самым превращает трансформацию из источника уязвимости в источник конкурентной устойчивости.

[8] Model Risk Management – управление модельным риском; AI-governance – управление ИИ-моделями.

Список источников

1. Институт внутренних аудиторов (IIA). Глобальные стандарты внутреннего аудита. Лейк-Мэри, Флорида: IIA, 2024 (The Institute of Internal Auditors. Global Internal Audit Standards) [на англ.].
2. Институт внутренних аудиторов (IIA). Тематические требования: кибербезопасность. Лейк-Мэри, Флорида: IIA, 2025. Вступает в силу 05.02.2026 (The Institute of Internal Auditors. Topical Requirements: Cybersecurity) [на англ.].
3. Комитет организаций – спонсоров Комиссии Тредвея (COSO). Корпоративное управление рисками: интеграция со стратегией и результативностью. COSO, 2017 (COSO. Enterprise Risk Management – Integrating with Strategy and Performance) [на англ.].
4. Международная организация по стандартизации (ISO). ISO 37000:2021 Руководство по корпоративному управлению организациями. Женева: ISO, 2021 (ISO. ISO 37000:2021 Governance of organizations – Guidance) [на англ.].
5. ГОСТ Р ИСО 31000–2019. Менеджмент риска. Принципы и руководство. М.: Стандартинформ, 2019 (Идентичен ISO 31000:2018) (ISO 31000:2018 Risk Management – Guidelines).
6. ISACA. COBIT 2019: цели управления и менеджмента. Шаумбург, Иллинойс: ISACA, 2018–2019 (ISACA. COBIT 2019 Framework: Governance and Management Objectives) [на англ.].
7. Национальный институт стандартов и технологий США (NIST). Рамочная основа по кибербезопасности (CSF) 2.0. Гейтерсберг, Мэриленд: NIST, 2024 (NIST. Cybersecurity Framework (CSF) 2.0) [на англ.].
8. ГОСТ Р ИСО/МЭК 27001–2021. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М.: Стандартинформ, 2021 (ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements).
9. ISO/IEC. ISO/IEC 27001:2022 Информационная безопасность, кибербезопасность и защита конфиденциальности – Системы менеджмента информационной безопасности – Требования. Женева: ISO/IEC, 2022 (ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements) [на англ.].
10. Базельский комитет по банковскому надзору. Принципы эффективной агрегации данных о рисках и отчетности по рискам (BCBS 239). Базель: Банк международных расчетов, 2013 (Basel Committee on Banking Supervision. Principles for effective risk data aggregation and risk reporting (BCBS 239) [на англ.].

Ознакомиться с презентацией

КАК ТЕХНОЛОГИИ ПОМОГАЮТ НАНИМАТЬ, ОБУЧАТЬ И РАЗВИВАТЬ СОТРУДНИКОВ ВНУТРЕННЕГО АУДИТА

Цифровая трансформация внутреннего аудита невозможна без развития новых компетенций специалистов. В этих условиях важно не только привлекать экспертов, но и формировать системную среду обучения и передачи знаний.

О.Н. ЩЁКОТОВ
Управляющий директор – заместитель директора Управления внутреннего аудита ПАО Сбербанк

Аннотация

Цифровая трансформация банковского сектора ставит перед внутренним аудитом задачу системного развития цифровых компетенций. Решение задачи путем привлечения в аудит опытных ИТ-специалистов (d-people) труднореализуемо в силу высокой конкуренции и стоимости таких кадров. В статье представлен альтернативный подход, применяемый Службой внутреннего аудита ПАО Сбербанк для решения проблемы найма d-people.

Ключевые слова: внутренний аудит, цифровые компетенции, ИТ-специалисты, наем d-people, интеллектуальный ассистент, адаптация сотрудников, база знаний, генеративный искусственный интеллект.

Коды JEL: M15, M42, O33.

Введение

Цифровизация вносит свои коррективы в привычные практики аудита. Усложнение процессов и рост объема данных, генерируемых цифровыми процессами, привели к необходимости перехода к цифровому аудиту, основанному на анализе 100% элементов (объектов, единиц) аудируемого процесса.

Для качественного анализа цифровых процессов необходимы цифровые аудиторы (d-people), обладающие навыками работы с большими данными и знаниями для проведения аудита моделей, участвующих в принятии решений. В этих условиях формирование и развитие цифровых компетенций становится ключевой задачей внутреннего аудита.

В настоящее время на рынке представлено более тысячи технологий по работе с данными. Даже при наличии понимания, какие цифровые компетенции необходимы, внутренний аудит сталкивается с рядом существенных ограничений при найме опытных d-people уровня middle и senior.

Опытные d-people:

- имеют узкую специализацию в отдельных технологиях и, как следствие, высокие ожидания по уровню вознаграждения;
- предпочитают удаленный режим работы;
- легко меняют работодателя в пользу более привлекательных условий труда и высокого вознаграждения.

Перечисленные факторы являются существенными ограничениями для найма d-people во внутренний аудит и приводят к необходимости увеличения расходов на функцию внутреннего аудита.

Альтернативный подход, применяемый Службой внутреннего аудита ПАО Сбербанк для решения проблемы найма d-people

Сбербанк является лидером цифровой трансформации, и вопрос наличия цифрового аудита должен был быть решен системно.

Комитет Наблюдательного совета по аудиту, проводя ежегодную оценку эффективности деятельности Службы внутреннего аудита ПАО Сбербанк, в том числе оценивает технологичность Службы и дает рекомендации по развитию компетенций Службы в области аудита рисков применения технологий.

Для решения проблемы найма d-people Службой внутреннего аудита ПАО Сбербанк был выбран альтернативный подход: вместо конкуренции за ограниченный пул дорогостоящих и узкоспециализированных ИТ-специалистов уровня middle/senior Службой успешно внедрен быстрый наем начинающих junior-специалистов и их ускоренный ввод в профессию. Наряду с этим была решена проблема удержания d-people: мы не удерживаем людей, а сохраняем их знания.

Технологии Службы внутреннего аудита ПАО Сбербанк, которые помогают нанимать, обучать и развивать сотрудников внутреннего аудита

1. «Бассейн новичков» – инструмент быстрого найма d-people уровня junior.

«Бассейн новичков» – это совместный проект Службы внутреннего аудита и HR-Службы, направленный на формирование устойчивого потока «теплых» кандидатов с базовыми цифровыми навыками (junior). Студенты/выпускники вузов с минимальными знаниями в области ИТ имеют реальную возможность получить работу.

Устойчивый поток кандидатов обеспечивается за счет стандартных требований на входе, так как кандидату необходимо успешно сдать только тесты HR и технический тест на знание SQL и Python. Пройти тесты может любой желающий.

Практика работы показала, что данная модель найма d-people выравнивает ожидания кандидатов и привлекательна для молодых людей, нацеленных на профессиональное развитие своих ИТ-навыков. На сегодняшний день «Бассейн новичков» – это 4,5 тыс. предодобренных кандидатов. Цикл подбора сотрудника на вакансию составляет 14 дней.

Массовый набор начинающих junior-специалистов позволил решить вопрос найма d-people без увеличения бюджета Службы.

2. Чат-бот-помощник hASK_ИИ – технология для быстрого ввода новичка в профессию.

Чат-бот-помощник hASK_ИИ доступен сотрудникам Службы в том числе для использования на мобильных телефонах. Общаясь с hASK_ИИ, новичок обращается к коллективному опыту десятков сотрудников Службы, ответы на вопросы формируются на основе базы знаний Службы с использованием модели GigaChat. Также для новичков сформулирован перечень вопросов, которые они обязательно должны задать помощнику hASK_ИИ.

Новичок может получить ответы на любые вопросы, касающиеся:
- роли Службы в корпоративном управлении;
- направлений работы и организационной структуры Службы;

- оформления необходимых доступов для работы в АС Банка и с корпоративной аналитической платформой;
- треков развития d-people Службы;
- нормативных документов Службы, методических рекомендаций, справочных ресурсов и других вопросов из программы адаптации новичков.

Онбординг (адаптация) новых сотрудников с hASK_ИИ позволил сократить срок ввода новых сотрудников в аудиторские проверки до 3–4 недель.

3. «База знаний СВА» – инструмент сохранения знаний и развития навыков.

«База знаний СВА» – это единое окно доступа к коллективным знаниям (экспертизе) Службы.

Ключевые характеристики инструмента:
- включает полную онтологию 30+ предметных областей. Онтология решает ключевые задачи: обеспечивает навигацию по базе знаний через иерархическую структуру категорий, позволяет устанавливать семантические связи между знаниями, обеспечивает единство терминологии и понятийного аппарата и служит основой для пополнения базы знаний новыми элементами;
- позволяет пользователям получить ответы от интеллектуального ассистента, генерирующего ответы на запросы пользователей с помощью генеративного искусственного интеллекта (GenAI).

Обязательное пополнение «Базы знаний СВА» по результатам каждой аудиторской проверки обеспечивает сохранение знаний и передачу их в дальнейшем от носителя знаний (даже если он уже уволился) новым сотрудникам Службы.

Таким образом, смещение фокуса внимания с задачи «удержать ИТ-специалиста любой ценой» на задачу «сохранить знания» позволяет повысить общий уровень экспертизы Службы в долгосрочной перспективе.

Заключение

Описанные выше технологии позволяют наращивать цифровые компетенции во внутреннем аудите без увеличения расходов, повышают масштабируемость компетенций Службы, снижают зависимость от дорогостоящих ИТ-специалистов и обеспечивают технологическую зрелость функции внутреннего аудита в условиях цифровой трансформации банковского сектора.

Список источников

1. Положение Банка России от 16.12.2003 № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах».
2. Информационное письмо Банка России от 01.10.2020 № ИН-06-28/143 «О рекомендациях по организации управления рисками, внутреннего контроля, внутреннего аудита, работы комитета совета директоров (наблюдательного совета) по аудиту в публичных акционерных обществах».
3. Гаврилова Т.А. Инженерия знаний. Модели и методы: Учебник для вузов / Т.А. Гаврилова, Д.В. Кудрявцев, Д.И. Муромцев. 5-е изд. СПб: Лань, 2022.

Ознакомиться с презентацией

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ МАНДАТА КОМИТЕТА ПО АУДИТУ ПУБЛИЧНОЙ КОМПАНИИ КОТИРОВАЛЬНОГО СПИСКА: УКРЕПЛЕНИЕ ДОВЕРИЯ К РЫНКУ КАПИТАЛА

Комитет по аудиту становится ключевым элементом системы доверия на рынке капитала, обеспечивая независимую оценку эффективности корпоративного управления и контрольной среды компании.

А.В. ШЕВЧУК
Исполнительный директор Ассоциации профессиональных инвесторов (АПИ)

Аннотация

В статье рассматривается цифровая трансформация мандата комитета по аудиту в публичных компаниях котировального списка как фактор укрепления доверия к рынку капитала. Автор анализирует, как новые технологии и ожидания инвесторов смещают фокус внимания комитета с верификации готовой отчетности на надзор за цифровой инфраструктурой ее формирования. На основе анализа международной практики (США, ЕС, Китай, Южная Корея, Индия) показана эволюция регулирования комитетов по аудиту в ответ на корпоративные скандалы и финансовые кризисы. Особое внимание уделяется проблемам независимости, вовлеченности и подотчетности комитетов в российских условиях, а также слабому взаимодействию с национальными институциональными инвесторами. В заключение предлагаются меры по повышению эффективности комитетов, включая реформу института независимых директоров, усиление их полномочий и использование инструментов цифровизации корпоративного управления.

Ключевые слова: комитет по аудиту, корпоративное управление, независимые директора, цифровая трансформация, финансовый надзор, рынок капитала.

Коды JEL: G34, M42, G38, O33.

Финансовая трансформация и ожидание инвесторов

Цифровая трансформация изменила ожидания инвесторов от комитета по аудиту: одно из направлений внимания инвесторов сместилось с верификации готовой финансовой отчетности на надзор за цифровой инфраструктурой ее формирования. Риск искажения может возникнуть не только из-за неверных суждений, предпосылок менеджмента и/или технической ошибки в проводках, но и из-за сбоя в цифровой среде по различным внешним и внутренним причинам. Новые риски – киберриски, риски качества данных, алгоритмические и платформенные риски, цифровая непрозрачность и риски третьих сторон – напрямую влияют на достоверность и полноту раскрытия информации. Возможности в области ERP-модернизации, автоматизации финансовых процессов, облачных вычислений и AI-аналитики подталкивают компании к трансформации финансовой системы. В международной практике развивается идея расширения мандата аудиторских комитетов

до контроля с его стороны за финансовой трансформацией через проработку основных 4 вопросов:

1. Стратегический план: обеспечение четкой дорожной карты трансформации.
2. Стандартизация и автоматизация: усиление контроля в цифровой финансовой функции.
3. Формирование кадрового резерва с необходимыми навыками и компетенцией.
4. Результаты: измерение успеха и обеспечение готовности к аудиту.

Новые возможности цифровой трансформации не меняют главного запроса инвесторов: им по-прежнему нужен системный подход. Их ключевой вопрос не изменился: обеспечивает ли комитет по аудиту реальное и достаточное покрытие стандартных и новых рисков и насколько он эффективен?

Важно отметить, что с точки зрения инвесторов эффективность комитета связана с его независимостью, и это один из центральных вопросов корпоративного управления. Практически все международные реформы последних 25 лет затрагивают вопросы усиления независимости – как структурной, так и экономической и поведенческой.

Международная практика развития мандата комитета по аудиту

Комитеты по аудиту являются ключевым элементом инфраструктуры финансовой отчетности, обеспечивая надзор за ее достоверностью, системой внутреннего контроля и взаимодействием с внешним и внутренним аудиторами.

В свою очередь, устойчивость рынка капитала и доверие инвесторов напрямую зависят от качества и надежности финансовой отчетности.

Международная практика демонстрирует поэтапное усиление регуляторного внимания к комитетам по аудиту как ответ на соответствующие кризисы корпоративного управления и финансовые скандалы. Поступательное развитие выражается в расширении мандата комитета по аудиту, усилении требований к их независимости и перераспределении ответственности.

В США главные кейсы-катализаторы серьезной реформы комитета по аудиту – это скандалы с отчетностью Enron (2001 год[9]) и WorldCom (2002 год). В обоих случаях – масштабные манипуляции и искажения отчетности, в кейсе Enron – сокрытие долгов и завышение прибыли, в кейсе WorldCom – завышение прибыли через капитализированные операционные расходы, результатом явились одни из крупнейших банкротств компаний. В результате 30 июля 2002 года принят закон Сарбейнса – Оксли (Sarbanes – Oxley Act, часто сокращается как SOX), который: 1) сделал комитет по аудиту обязательным для публичных компаний; 2) усилил требования к независимости его членов; 3) закрепил прямую подотчетность внешнего аудитора комитету, а не менеджменту.

В ЕС один из самых влиятельных кейсов – скандал вокруг Parmalat (2003), когда выяснилось, что активов на примерно 14–15 млрд евро фактически не существовало, фальсифицировались банковские подтверждения и использовались офшорные структуры для скрытия долгов, а ключевой расчетный счет в Bank of America оказался поддельным. В результате **в ЕС в 2006 году была принята** Директива 2006/43/ЕС**, устанавливающая единые стандарты аудиторских проверок, квалификации аудиторов и надзора за ними.** Директива закрепила, что для компаний общественного интереса комитет по аудиту обязателен, комитет должен состоять из неисполнительных директоров и минимум один член комитета обязан обладать знаниями в бухгалтерском учете или аудите. Кроме того, закрепляются функции комитета: 1) контроль

[9] U.S. Senate Permanent Subcommittee on Investigations (2002). The Role of the Board of Directors in Enron»s Collapse. Washington, DC: U.S. Government Printing Office.

финансовой отчетности; 2) надзор за внутренним контролем и риск-менеджментом; 3) надзор за обязательным аудитом; 4) контроль независимости аудитора.

Финансовый кризис 2008 года в том числе показал, что усиление роли комитета недостаточно, компании были разрушены из-за реализовавшихся рисков, моделей оценки и слабого надзора со стороны советов директоров. Крах банков и финансовых институтов (например, Lehman Brothers) продемонстрировал, что отчетность формально соответствовала стандартам, но реальные риски были скрыты. Советы директоров не понимали сложных финансовых инструментов, а комитеты по аудиту концентрировались исключительно на бухгалтерских проводках, а не на моделях оценки активов, которые по сути не оспаривались в ходе рассмотрения суждений менеджмента. После кризиса во многих юрисдикциях (ЕС, Великобритания, США, Азия) мандат комитетов расширился: 1) дополнен подход к мониторингу системы управления рисками в части рассмотрения стресс-сценариев, расширенному контролю системы через политику информирования нарушений и управление рисками мошенничества; 2) усилен контроль оценочных суждений, включая критическое оспаривание позиции менеджмента; 3) дополнена практика взаимодействия с аудитором: обсуждение ключевых аудиторских вопросов, встречи без менеджмента и оценка качества процесса аудита (помимо заключения). Как пример, **кризис стал прямым драйвером реформы и обновления директивы об аудите в Европейском союзе** (Регламент (EU) No 537/2014). Регламент дополняет и конкретизирует положения Директивы 2006/43/ЕС, усиливая роль комитетов по аудиту в процессе выбора и контроля аудиторов. Устанавливаются ограничения на оказание аудиторскими фирмами неаудиторских услуг, вводятся требования к ротации аудиторских компаний, структуре аудиторского отчета и дополнительной отчетности для комитетов по аудиту.

После ситуации с Wirecard в 2020 году (когда значительная часть прибыли компании не могла быть подтверждена, аудиторы не получили достаточных доказательств существования денежных средств и многие операции с третьими лицами не были проверяемы) по сути **произошел еще один этап усиления ответственности и практического контроля для комитетов по аудиту в части качества надзора после реформы 2014 года в ЕС**. Кроме того, в Германии данный кейс привел к реформе финансового надзора BaFin. В частности, были усилены требования к экспертизе в комитете по аудиту, введено обязательство минимум одного эксперта по бухгалтерскому учету и одного эксперта по аудиту, при этом экспертиза должна быть подтверждаемой и релевантной.

В странах Азии под влиянием международного рынка портфельных инвестиций и, соответственно, мировых кризисов также внедрялись аналогичные подходы к функционированию комитетов по аудиту. С другой стороны, с учетом особенностей регионов в части высокой концентрации собственности среди акционерного капитала за последние несколько лет произошли интересные изменения, направленные в первую очередь на решение проблемы независимости комитетов по аудиту (Китай, Южная Корея), а также добавление отдельных блоков дополнительной компетенции (Индия).

В Китае произошла наиболее мягкая реформа института независимых директоров в сентябре 2023 года с переходным периодом в 1 год для адаптации компаний. Наиболее важные нововведения, которые затрагивают комитет по аудиту:

- ограничение юридической ответственности независимых директоров: в регулировании отмечается, что, если независимые директора выполнили свои основные обязанности и все же не обнаружили проблем до подписания документа или если компании, акции которых котируются на бирже, умышленно скрывают нарушения законодательства, независимые директора могут быть освобождены от штрафных санкций;
- предоставление независимым директорам полномочий самостоятельно привлекать консультантов/экспертов для проведения аудита, консультаций или анализа конкретных вопросов, касающихся компаний, акции которых котируются на бирже;

– требование к компаниям, акции которых котируются на бирже, обеспечивать необходимые условия труда и кадровую поддержку, позволяющие независимым директорам выполнять свои обязанности, а также предоставлять им такое же право на информацию, как и другим директорам, не являющимся независимыми.

Безусловно, самые важные изменения – это ответственность и ресурсы, предоставляемые независимым директорам, в том числе членам комитета по аудиту, в то же время эксперты отмечают проблему независимости в целом совета директоров и, соответственно, комитета. На практике крупные акционеры или фактические контролирующие лица сохраняют значительное влияние при выдвижении кандидатур независимых директоров. Это создает проблему обеспечения подлинной независимости директоров от крупных акционеров при выполнении ими своих обязанностей.

В Южной Корее пошли существенно дальше в части решения проблемы независимости и сосредоточились на членах комитета по аудиту – независимых директорах, которые выбираются по отдельной схеме. Голосование за независимых директоров, которых выбирают как будущих членов комитета по аудиту, осуществляется с ограничением права голоса крупнейшего акционера и связанных с ним лиц в размере 3% голосующих акций. Согласно новому законодательству (подход будет применяться с 23 июля 2026 года), компании, акции которых котируются на бирже и активы которых составляют 2 трлн вон или более, обязаны создать комитет по аудиту, при избрании которого совокупная доля голосов крупнейшего акционера и связанных с ним лиц ограничена 3%. Это уже уточненная реформа комитета по аудиту, так как до поправок 2025 года ограничение в 3% не обеспечивало выбор именно независимых директоров и на практике не препятствовало избранию внешних, но не независимых кандидатов.

В Индии в 2015 году регулятор рынка капитала (SEBI) значительно расширил функции комитета по аудиту, все сделки с заинтересованностью требуют предварительного одобрения комитета по аудиту, и голосуют только независимые члены комитета. Кроме того, компания обязана создать систему выявления правонарушений с прямым доступом к председателю комитета по аудиту, у комитета есть полномочия по расследованию (запрос информации у сотрудников компании, привлечение внешних экспертов и инициирование проверок) и стандартные обязанности надзора за внутренним контролем и риск-процессами.

Соответственно, в международной практике мы видим существенные постоянные изменения регулирования комитетов по аудиту, который является отдельным важным объектом внимания как акционеров, инвесторов, так и регуляторов, особенно в компаниях, имеющих листинг на биржах. Следует также выделить различные подходы к решению проблем независимости комитетов и определить их место в системе принятия решений.

Отдельный вопрос, требующий особого внимания, – это обязательность решений комитетов по аудиту. Мы видим наиболее строгий подход в США с обязательным положительным заключением комитета определенного перечня вопросов (в первую очередь в отношении внешнего аудитора) по результатам внедрения SOX. Но также существуют и более мягкие подходы (на примере юрисдикции Гонконга): если совет директоров не принимает рекомендацию комитета по аудиту, то должно быть раскрытие информации с объяснением/обоснованием позиции обеих сторон, то есть почему Комитет по аудиту рекомендует так, а совет директоров считает и решает по-другому. Вопросы обязательности решений комитета являются не менее важными составляющими эффективности данного органа.

Почему рассматриваются комитеты котировальных списков бирж?

Котировальные списки первого и второго уровней рассматриваются как ориентир повышенных стандартов корпоративного управления, поскольку для эмитентов данных уровней установлено требование: большинство членов комитета по аудиту должны составлять независимые директора.

Институциональная независимость в сочетании с профессиональной компетентностью и активной позицией членов комитета является ключевым механизмом обеспечения доверия инвесторов и устойчивости рынка капитала.

Мы также видим из международной практики, что наибольшее внимание регулирования сосредоточено на компаниях с листингом.

Потенциал и проблемы в российских условиях

Цифровая трансформация не устранила институциональные проблемы корпоративного управления: недостаток реальной независимости и профессиональной вовлеченности директоров является катализатором (мультипликатором) уязвимостей в отчетности и финансово-хозяйственной деятельности компаний.

По факту институциональные инвесторы в условиях ухода/заморозки международного капитала существенно ослабили свое и так небольшое влияние на комитеты по аудиту. Встречи с инвесторами независимых директоров членов комитета по аудиту перестали практиковаться. Локальные/национальные инвесторы в большинстве компаний котировального списка имеют крайне ограниченную долю во free-float, а также сами не понимают и не реализуют инструменты взаимодействия с комитетами. Соответственно, комитеты не ощущают какой-либо поддержки и интереса/внимания со стороны инвесторов к своей работе, что также сказывается на качестве исполнения ими своих фидуциарных обязанностей.

В восприятии инвесторов в текущей национальной практике потенциал комитета по аудиту не реализован: в большинстве компаний котировальных списков организатора торгов (биржи) комитеты не являются по факту основными заказчиками внешнего и внутреннего аудиторов и независимым надзором за управлением рисками и системой внутреннего контроля.

Наиболее распространенная практика – когда менеджмент предлагает комитету по аудиту кандидатуру внешнего аудитора. Таким образом, комитет не контролирует риск зависимости аудитора от менеджмента в условиях потенциального конфликта интересов. По наблюдениям инвесторов, цена аудита и формальные критерии (например, сертификаты) за последние несколько лет становятся предопределяющими факторами выбора аудиторов. комитет также не погружается в проблематику процесса внешнего аудита и, как правило, не контролирует процесс подписания отчетности (обсуждение ключевых суждений с менеджментом и внешним аудитором, в том числе отдельно от менеджмента).

Простой краткий опрос автором партнеров крупнейших аудиторов показывает крайне слабое влияние комитета по аудиту на их работу, их главный заказчик – это менеджмент во главе, как правило, финансового директора и/или главного бухгалтера.

Качество поддержки комитетом по аудиту независимой функции внутреннего аудита неизвестно инвесторам на фоне низкой прозрачности и подотчетности комитетов компаний даже котировальных списков и отсутствия содержательных встреч инвесторов хотя бы с председателями комитетов и/или независимыми членами. Например, изучение отчетности новых компаний, вышедших на IPO за последние 3–4 года, косвенно свидетельствует о формальном

подходе к организации функции внутреннего аудита, новые руководители подразделений назначаются, как правило, из сотрудников компании без соответствующего опыта во внутреннем аудите, что также усиливает риски зависимости функции от менеджмента и автоматически снижает роль и вес комитета по аудиту в системе корпоративного управления.

Как уже отмечалось выше, одна из причин непрозрачности комитета по аудиту котировальных списков (по сути, независимых директоров) – проблема отсутствия практики регулярного взаимодействия портфельных инвесторов – крупных национальных институциональных инвесторов, например при подготовке и проведении годовых общих собраний акционеров компаний. Институциональные инвесторы не проявляют должного внимания и не оказывают поддержки независимым директорам, так как считают свои возможности влияния ограниченными в условиях низких значений голосующего free-float компаний и доли самих национальных институционалов в акционерном капитале компаний. Независимые директора, в свою очередь, находясь в том числе под существенным влиянием основных акционеров в условиях концентрированной собственности, скептически относятся к контактам с инвесторами.

Предложения по усилению эффективности комитета по аудиту

Цифровизация активного корпоративного управления (например, создание соответствующей платформы корпоративных действий на уровне бирж или НРД) формирует потенциал для консолидации миноритарных акционеров, локомотивом которых могут выступать профессиональные национальные инвесторы. Возможно, при должном темпе развития практики ответственного инвестирования для таких инвесторов могут быть рассмотрены экономические стимулы, в том числе со стороны регулирования деятельности профессиональных участников рынка капитала (например, соответствующие возможности по дополнительной аллокации или снижение определенной регуляторной нагрузки при условии должного раскрытия информации профессиональным участником).

В условиях ограниченного влияния голосующего free-float даже в компаниях котировального списка организатора торгов имеет смысл обсуждать соответствующую реформу института независимых директоров с опорой в том числе на опыт Индии (двухэтапное голосование: мажоритарное и миноритарное голосование по определенным вопросам и их распространение на выборы независимых директоров), Южной Кореи (ограничение голосования мажоритарного акционера и связанных лиц) и собственный национальный накопленный опыт кумулятивного голосования за последние 25 лет.

Комитет по аудиту должен быть сформирован полностью из независимых директоров для компаний котировальных списков, институциональные инвесторы должны активно взаимодействовать с членами комитетов, повышая подотчетность и усиливая роль комитета внутри компании. Как минимум председателем комитета компании котировального списка должна быть публичная фигура. Независимые директора должны осознавать свои обязанности по общению с акционерами в рамках своей компетенции и с учетом всех особенностей регулирования в области инсайдерской информации (возможно, требуются дополнительные совместные обучающие встречи со стороны регулятора и/или организатора торгов, представителей инвесторов и независимых директоров).

Опираясь на международную и национальную практику, можно рассмотреть несколько опций по усилению позиций и эффективности комитета по аудиту внутри компаний, например, определенного котировального списка:

- обязательное положительное заключение комитета по аудиту при рассмотрении советом директоров определенного набора вопросов[10] (опыт США и российский опыт во время реформы РАО ЕЭС России, когда без положительного заключения комитета совет директоров энергохолдинга не рассматривал вопрос, компетенция которого затрагивалась соответствующим комитетом);
- облегченная модель (Гонконг): если совет директоров не принимает рекомендацию комитета по аудиту, то должно быть раскрытие информации с объяснением/обоснованием позиции обеих сторон;
- возможность привлекать независимых от компании и существенных акционеров экспертов с соответствующим необходимым бюджетированием расходов (опыт реформы независимых директоров в материковом Китае);
- обязательное очное рассмотрение определенных вопросов и минимальный порог очных заседаний в год: 4 заседания, в том числе без участия менеджмента с внешними и внутренними аудиторами.

Цифровизация системы корпоративного управления (как пример – электронное голосование, гибридные формы собраний/заседаний, механизмы консолидаций и взаимодействия с инвесторами) может также выступать инструментом раскрытия потенциала комитета по аудиту.

Список источников

1. Закон Сарбейнса – Оксли 2002 года (Sarbanes-Oxley Act of 2002) – федеральный закон США о реформе корпоративной отчетности и аудита. Вашингтон, 2002.
2. Европейский парламент и Совет Европейского союза. Директива 2006/43/ЕС от 17 мая 2006 года об обязательном аудите годовой и консолидированной финансовой отчетности // Официальный журнал Европейского союза. 2006.
3. Европейский парламент и Совет Европейского союза. Регламент (ЕС) № 537/2014 от 16 апреля 2014 года о специальных требованиях к обязательному аудиту организаций общественного интереса // Официальный журнал Европейского союза. 2014.
4. Организация экономического сотрудничества и развития (ОЭСР). Принципы корпоративного управления G20/ОЭСР. Париж: ОЭСР, 2015.
5. Комитет спонсорских организаций Комиссии Тредвея (COSO). Управление рисками организации: интеграция со стратегией и эффективностью деятельности. Нью-Йорк: COSO, 2017.
6. Совет по финансовой стабильности. Тематический обзор корпоративного управления рисками. Базель: Financial Stability Board, 2013.
7. Кляйн Э. Комитет по аудиту, характеристики совета директоров и управление прибылью // Журнал экономики бухгалтерского учета. 2002. Т. 33, № 3. С. 375–400.

[10] Список возможных вопросов:
- рекомендации по выбору (включая организацию проведения комитетом по аудиту отбора/конкурса) внешнего аудитора;
- согласование утверждения договора с внешним аудитором и акта выполненных работ;
- согласование раскрытия промежуточной/годовой МСФО и РСБУ отчетности;
- утверждение кандидатуры, трудового договора, бюджета и плана работы подразделения внутреннего аудита;
- сделки с заинтересованностью, утверждение результатов независимой оценки акций компании и/или цены выкупа акций компании.

8. Бизли М., Карчелло Дж., Хермансон Д., Нил Т. Надзор комитетов по аудиту и качество финансовой отчетности // Современные исследования бухгалтерского учета. 2009. Т. 26, № 1. С. 65–122.
9. Дезорт Ф., Хермансон Д., Аршамбо Д., Рид С. Эффективность комитетов по аудиту: обзор эмпирических исследований // Журнал литературы по бухгалтерскому учету. 2002. Т. 21. С. 38–75.
10. Совет по ценным бумагам и биржам Индии (SEBI). Требования к листингу и раскрытию информации. Мумбаи: SEBI, 2015.

Ознакомиться с презентацией

ВЫЗОВЫ И СЛОЖНОСТИ В РАБОТЕ КОМИТЕТА ПО АУДИТУ И РИСКАМ В НЕФИНАНСОВОМ СЕКТОРЕ: ЭВОЛЮЦИЯ РОЛИ В СИСТЕМЕ КОНТРОЛЯ И УПРАВЛЕНИЯ

Роль комитетов по аудиту и рискам существенно расширяется: сегодня они рассматривают не только вопросы финансовой отчетности, но и стратегические, технологические и киберриски.

А.А. САЛТЫКОВА
Независимый директор, член советов директоров ряда крупных российских компаний

Аннотация

Статья посвящена эволюции роли комитета по аудиту и рискам совета директоров компаний нефинансового сектора в России[11]. Отмечены такие аспекты, как перезагрузка корпоративной повестки под влиянием ряда внешних факторов, возрастающая сложность бизнеса, неопределенность и волатильность, трансформация запроса внешних и внутренних пользователей. На уровне комитета произошел переход к проактивной повестке, использованию кросс-функционального подхода, интеграции всех линий защиты, повысилась вовлеченность комитета и нагрузка на него.

В статье рассмотрены некоторые актуальные вопросы и вызовы, которые стоят перед комитетом в 2026 году в связи с произошедшими и идущими внешними и внутренними изменениями, включая вопросы обеспечения устойчивости бизнеса, оптимизации деятельности, тщательного мониторинга ключевых рисков, повышения требований к инвестициям и рисков возможного технологического отставания. Затронута проблематика, связанная с информационными технологиями как относительно новой сферой особого внимания комитета. Рассмотрены вопросы обеспечения достоверности финансовой отчетности, развития правил и компетенций. Приведены примеры возможных мер по развитию института комитетов по аудиту и рискам и повышению эффективности его работы на уровне компании.

Ключевые слова: кибербезопасность, корпоративное управление; комитет по аудиту и рискам; искусственный интеллект; нефинансовая отчетность; управление рисками; финансовая отчетность; устойчивость бизнеса.

Коды JEL: G34, M42, D81, O33, L21.

Корпоративное управление в России прошло стремительный путь развития за последние три десятка лет. За это время практика создания и работы комитетов по аудиту и рискам советов директоров в нефинансовом секторе формировалась опережающими темпами по сравнению с законодательством. Комитеты в России эволюционировали от создаваемых в инициативном порядке, для выхода на зарубежные рынки капитала, до требуемых правилами листинга и Кодексом корпоративного управления, рекомендуемых

[11] Вопросы, затронутые в этой статье, предлагается рассматривать как развитие тем, рассмотренных в статье «Текущие вызовы и некоторые особенности работы комитетов по аудиту в финансовом и нефинансовых секторах».

регуляторами, и, наконец, формируемых в силу требований Федерального закона «Об акционерных обществах». Комитет по аудиту является единственным комитетом совета директоров публичного акционерного общества, прямо предусмотренным требованиями указанного закона. Комитет по аудиту создается для предварительного рассмотрения вопросов, связанных с контролем за финансово-хозяйственной деятельностью публичного общества, включая оценку независимости аудиторской организации публичного общества и качества проведения аудита бухгалтерской (финансовой) отчетности. Кодексом корпоративного управления определены основные задачи комитета по аудиту в 4 областях: (бухгалтерской) финансовой отчетности, управления рисками и внутреннего контроля, проведения внутреннего и внешнего аудита, противодействия недобросовестным действиям работников общества и третьих лиц.

Комитет по управлению рисками на практике в нефинансовых организациях часто не создается отдельно, вопросы управления рисками рассматривает комитет по аудиту. В этой связи в данной статье комитет именуется комитетом по аудиту и рискам.

Фокус деятельности комитета определяется приоритетами общества, развитием внешней среды, взглядами советов директоров, комитета, исполнительного руководства. Геополитические, экономические, технологические риски, а также кадровые вопросы остро стоят на повестке, влияя на конкурентоспособность компаний, возможности и перспективы роста и технологического развития, обеспечение устойчивости бизнеса, цепочек поставок, критической инфраструктуры, кибербезопасности, эффективность работы, выявление оптимальных моделей и ресурсов для развития.

Технологические риски, включая киберриски, применение искусственного интеллекта (ИИ), вошли в сферу рассматриваемых комитетом по аудиту и рискам вопросов ввиду их значимости для обществ, требуя особого внимания комитета и развития компетенций. По оценкам Всемирного экономического форума (ВЭФ) геоэкономический риск, риски ложной и искаженной информации, а также киберриски заняли первое, второе и шестое места соответственно среди самых значимых рисков в прогнозе 2026 года на горизонте следующих 2 лет. Экономические и геополитические риски (геоэкономическая конфронтация, экономический спад, инфляция, сдутие пузыря переоцененных активов, нарушение работы критической инфраструктуры) показали наибольший прирост по значимости на двухлетнем горизонте. На десятилетнем горизонте риски ложной и искаженной информации, отрицательных последствий применения технологий ИИ, а также киберриски, по данным ВЭФ, занимают четвертое, пятое и восьмое места соответственно. Стала приоритетной и общепризнанной повестка, связанная с окружающей средой, социальной ответственностью, что привело к появлению специальной отчетности, которая может рассматриваться комитетом.

Запросы пользователей на прозрачность и открытость отчетной информации стали стимулом для стремительного развития правил финансовой отчетности как по РСБУ, так и по МСФО, повышения ее информативности, применения новых оценок, сопоставимости отчетности и привели к ее усложнению и увеличению объема. Показатели финансовой отчетности, включая и оценку статей, и раскрытие информации, тесно связаны со стратегией и рисками, взглядом руководства на управление и анализ бизнеса, а не только с исторической информацией. Эти изменения потребовали от компаний и комитетов по аудиту и рискам времени и усилий в оценке и применении изменений и кросс-функционального подхода. Усилена работа с внешним и внутренним аудитом. Комитету важно понимание не только финансовых аспектов, но и, например, того, как функционирует все время усложняющийся бизнес и его сегменты, каковы внешние рынки сбыта с учетом растущей волатильности и неопределенности, есть ли угроза технологического отставания, нужна ли адаптация системы управлениями инвестициями, каковы

узкие места в системе поставок, какое влияние на деятельность компании и кибербезопасность могут оказать услуги третьих лиц и другое.

Кибербезопасность и риски, связанные с информационными системами, стали вопросом, на который обращает повышенное внимание совет директоров, в мире этот вопрос часто включается для более детальной проработки в компетенцию комитета по аудиту и рискам. Внимание к нему будет только расти. Это направление требует наращивания новых компетенций и корректировки применяемых подходов.

Повысились требования и ожидания внутри компаний и внешних пользователей в отношении системы управления рисками и внутреннего контроля, ее надежности и эффективности, а также качества корпоративного управления. Можно ожидать, что внешние пользователи будут все больше заинтересованы во внешних оценках эффективности работы этих систем. Система трех линий, включая внутренний аудит, стала понятной практикой. В России получила признание профессия внутреннего аудитора, который является теперь «глазами» совета директоров и комитета по аудиту и рискам, произошло принятие разграничения между внутренним контролем и внутренним аудитом.

В 2026 году на повестке комитета по аудиту и рискам, помимо традиционного набора вопросов, есть ряд аспектов, которые могут потребовать особого внимания. Обеспечение устойчивости бизнеса ввиду его усложнения, внешней неопределенности и волатильности потребует особого внимания к управлению рисками, особенно ключевыми, установлению и соблюдению риск-аппетита, подходам к планированию и реагированию. Комитет совместно с менеджментом может перейти к более частому рассмотрению вопроса на своих заседаниях. На повестке советов директоров и комитета остро стоит вопрос исполнения стратегии, важно, чтобы ключевые риски и риск-аппетит были увязаны со стратегией, находясь на радаре комитета по аудиту и рискам. Стресс-тестирование и планы антикризисных мероприятий могут быть востребованы больше, чем обычно. В отношении кибербезопасности модели и планы реагирования стали привычной практикой, и она может быть успешно распространена в нефинансовых организациях на другие аспекты деятельности.

Кибербезопасность, вопросы ИТ-систем, использования ИИ требуют внимания со стороны совета директоров и могут прорабатываться на комитете по аудиту и рискам. По разным оценкам, в мире доля комитетов по аудиту, которые имеют в зоне прямой ответственности или глубоко вовлечены в рассмотрение вопросов кибербезопасности, превышает 60%. В последнее время опубликовано несколько тематических руководств для внутреннего аудита в этой и сопряженных областях. Имеющая место в последние годы стремительная трансформация в области информационных технологий и смена провайдеров также может представлять риск с точки зрения кибербезопасности и нуждается в мониторинге. Использование ИИ включает рассмотрение его применения в более широком контексте, чем только с учетом формализованных ограничений внутри компании.

Следует отметить, что в мире растет обеспокоенность и понимание рисков со стороны третьих лиц, оказывающих услуги компании. Например, ИТ-компания, обслуживающая многих крупных клиентов или целую отрасль экономики, может быть целью кибермошенников для нанесения ущерба ее клиентам, а качество и устойчивость сервиса ИТ-компании может быть критично для бизнес-процессов клиентов.

Проектируемые изменения в правилах учета и финансовой отчетности, применимом законодательстве, включая отраслевое, правилах раскрытия информации пользователям на рынках ценных бумаг, включая нефинансовую информацию, полнота и качество информации, своевременность предоставления ее пользователям также требуют внимания со стороны

комитета. Например, применение ФСБУ 9/2025 «Доходы организации» в будущем вместе с проектируемым ФСБУ «Расходы», МСФО (IFRS) 18, новые правила представления финансовой отчетности в государственный информационный ресурс бухгалтерской (финансовой) отчетности, вопросы полноты раскрытия информации для пользователей, ее взаимосвязанности и качества находятся на повестке комитета. Карта уверенности в отношении такой информации и работа со сторонами, предоставляющими такую уверенность, тоже важная часть работы комитета.

Дополнительной областью внимания для комитета является кадровый вопрос, особенно в подразделениях внутреннего аудита, аудита ИТ-систем, управления рисками, требуют внимания вопросы преемственности и работы с возрастным сдвигом, в том числе в отношении состава комитета.

Комитет по аудиту и рискам стал проактивным, кросс-функциональным «отрядом специального назначения», имеющим стратегическую важность для успешной деятельности общества и совета директоров. Для повышения его эффективности с учетом особенностей деятельности компаний советом директоров, менеджментом и председателем комитета могут быть применены такие меры, как программы развития и обучения, страхования ответственности, введение системы вознаграждения членов комитета и совета директоров с учетом растущей нагрузки на комитет и его членов, применение ИИ для поддержки деятельности комитета, выделения резерва для привлечения к работе экспертов по мере необходимости, повышение требований к уровню дискуссии и подготовке материалов, создание дополнительных (под) комитетов с учетом нагрузки, ее перераспределение между существующими комитетами, проведение совместных заседаний комитетов и другие. Кроме того, существует ряд возможных институциональных мер, которые могут быть рассмотрены на различных уровнях. Следует отметить, что актуальные комплексные исследования проблематики комитета по аудиту и рискам и других комитетов советов директоров в России редки и могут быть полезны для оценки существующего ландшафта и планирования мер по развитию корпоративного управления.

Список источников

1. Федеральный закон от 26.12.1995 № 208-ФЗ «Об акционерных обществах» (с последующими изменениями и дополнениями).
2. Информационное письмо Банка России от 01.10.2020 № ИН-06-28/143 «О рекомендациях по организации управления рисками, внутреннего контроля, внутреннего аудита, работы комитета совета директоров (наблюдательного совета) по аудиту в публичных акционерных обществах».
3. Письмо Банка России от 10.04.2014 № 06-52/2463 «О Кодексе корпоративного управления».
4. Письмо Банка России от 15.09.2016 № ИН-015-52/66 «О положениях о совете директоров и о комитетах совета директоров публичного акционерного общества».
5. Приказ Федерального агентства по управлению государственным имуществом от 20.03.2014 № 86 «Об утверждении Методических рекомендаций по организации работы комитетов по аудиту советов директоров акционерных обществ с участием Российской Федерации».
6. Обзор финансовой стабильности. II–III кварталы 2025 года. Банк России.
7. Мониторинг предприятий. Февраль 2026. Банк России.
8. Топ-50 компаний: испытание на прочность. Анализ динамики финансовых показателей 50 крупнейших российских публичных нефинансовых компаний (топ-50) в 2024 году и первом полугодии 2025 года. АКРА.
9. Обзор практик корпоративного управления. Портрет совета директоров. Аналитическое исследование НОКС. 2024.

10. Национальный доклад по корпоративному управлению. Выпуск XIV. Национальный совет по корпоративном управлению. 2025.
11. CODE RED 2026: Актуальные киберугрозы для российских организаций. Positive Technologies.
12. Тренды атак в 2026 году. Positive Technologies.
13. Руководящие указания по организации внутреннего аудита. ПНСТ 1034–2025.
14. Global Risks Report 2026, 21st Edition, World Economic Forum.
15. Кибербезопасность. Тематические требования. Институт внутренних аудиторов.
16. Кибербезопасность. Руководство по применению тематических требований. Институт внутренних аудиторов.
17. Взаимоотношения с третьими сторонами. Тематические требования. Институт внутренних аудиторов.
18. Взаимоотношения с третьими сторонами. Тематические требования. Руководство пользователя. Институт внутренних аудиторов.
19. Organizational Behaviour. Topical Guidance. IIA.
20. Organizational Behaviour. Topical Guidance. User Guide. IIA.
21. 2026 Global Risk in Focus.
22. Gartner Top Strategic Technology Trends for 2026.
23. 2025 Audit Committees Survey Insights. Key Challenges, Concerns and Priorities. KPMG.
24. 2026 Audit Committee Priorities: Navigating Complexity and Change. EY Center for Board Matters.

Ознакомиться с презентацией

НОВЫЕ ФОКУСЫ СИСТЕМЫ ВНУТРЕННЕГО КОНТРОЛЯ И ВНУТРЕННЕГО АУДИТА В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ И КАДРОВОГО ДЕФИЦИТА

Цифровизация бизнес-процессов приводит к появлению новых объектов внутреннего аудита – от управления данными до контроля алгоритмов и автоматизированных систем принятия решений.

А.В. ДАВЫДОВА
Руководитель группы внутреннего аудита, анализа и контроля рисков, ООО «Технологии Доверия – Консультирование»

АННОТАЦИЯ

Система внутреннего контроля организаций в последние несколько лет подвержена достаточно существенным изменениям. Ключевые факторы таких изменения – цифровая трансформация бизнес-процессов и кадровый дефицит. В статье рассматриваются новые области и объекты аудита, которые появились в связи с цифровизацией системы внутреннего контроля. Подчеркивается важность переосмысления фокуса внимания комитетов по аудиту, руководства организаций и функции внутреннего аудита в обеспечении надежности и эффективности системы внутреннего контроля в контексте цифровой трансформации бизнес-процессов.

Ключевые слова: система внутреннего контроля, внутренний аудит, риски, информационные технологии, цифровизация, цифровая трансформация.

Коды JEL: M42, M15, O33, D81.

Система внутреннего контроля финансовых и нефинансовых организаций претерпевает в последние годы значительные изменения. Ключевыми факторами, оказывающими влияние на трансформацию системы внутреннего контроля, являются цифровизация бизнес-процессов организации и кадровый дефицит.

Бурное развитие технологий кардинальным образом меняет подход к сложившимся рабочим практикам в финансовых и нефинансовых организациях. Цифровизация позволяет увеличивать производительность, повышать качество продукции, дает конкурентные преимущества. Оказывая влияние на бизнес-процессы, цифровая трансформация неизбежно влияет на выстроенную систему внутреннего контроля организации, которая также становится более автоматизированной.

Цифровизация системы внутреннего контроля также помогает решить проблему кадрового дефицита. Ручные контрольные процедуры заменяются на автоматические и параллельно с этим происходит постепенное смещение фокуса с последующих контролей на предварительные (предупреждающие).

Фонд внутреннего аудита (Internal audit foundation) на ежегодной основе проводит исследование о ключевых рисках, которые в настоящий момент, по мнению внутренних аудиторов из различных стран мира, стоят перед их организацией. Если проанализировать исследования

за 2024–2026 годов, то видно, что топ-5 рисков на глобальном уровне в последние 3 года остаются неизменными:

1. Риски информационной безопасности.
2. Риски обеспечения непрерывности деятельности бизнеса.
3. Риски цифровой трансформации бизнеса.
4. Регуляторные риски.
5. Риски, связанные с человеческим капиталом.

При этом по результатам тех же исследований видно, что фокус внимания внутренних аудиторов на сегодняшний день по-прежнему в значительной степени направлен на традиционные области аудита, связанные с корпоративным управлением, финансовой отчетностью, управлением ликвидностью, мошенничеством. Вопросы, связанные с информационной безопасностью и обеспечением непрерывности деятельности бизнеса, также начинают прочно входить в текущую повестку внутренних аудиторов.

Риски, связанные с цифровой трансформацией бизнеса, пока не в полной мере подхватываются внутренними аудиторами. Тем не менее цифровизация бизнес-процессов и системы внутреннего контроля привносят новые риски и новые объекты аудита. Можно выделить семь ключевых областей, на которые в первую очередь стоит обратить внимание.

1. Замена ручных контрольных процедур автоматическими помогает повысить эффективность и скорость выполнения процедур, снижает зависимость организации от наличия рабочей силы. Принято считать, что автоматическая контрольная процедура всегда работает лучше и точнее, чем человек. Человек может ошибиться, информационная система работает по заданному алгоритму. Однако если никто заранее не протестировал корректность работы алгоритма, то автоматизированное решение может содержать ошибку. Ошибка будет повторяться в 100% случаев работы контрольной процедуры, что может оказать существенное влияние на надежность системы внутреннего контроля.
2. Цифровизация бизнес-процессов и зависимость течения бизнес-процесса от информационных систем повышают важность эффективной работы общих средств контроля за информационными технологиями. Например, процессы предоставления доступа к тем или иным информационным системам и базам данных, процессы своевременного отзыва ранее предоставленных прав, процессы управления изменениями в информационных системах. Общие средства контроля за информационными технологиями представляют собой фундамент системы внутреннего контроля в эпоху цифровизации.
3. Важным аспектом внимания становится подход к разделению ролей и полномочий в информационных системах. В любой крупной финансовой и нефинансовой организации насчитывается не один десяток систем. Поэтому важно понимать, у какого работника к какому функционалу есть доступ. Особое внимание необходимо уделить разделению ролей и полномочий на пересечении различных систем.
4. Исторически организации не придавали должного значения качеству данных, которые на ежедневной основе формировались и накапливались в информационных системах. На сегодняшний день качество данных в информационных системах – это отдельный, новый объект внимания внутреннего аудита. В эпоху активного использования дашбордов для аналитики и ежедневного принятия управленческих решений сложно переоценить важность наличия корректной и достоверной информации.
5. Мастер-данные также становятся важным объектом аудита. Учитывая многообразие используемых организациями систем и настроенные между ними интерфейсы по передаче данных, важно понимать какая система является первоисточником данных, каким образом организована система внутреннего контроля вокруг обеспечения целостности и эффективного управления мастер-данными.

6. В последнее время достаточно широко начинают использовать новые технологии в бизнес-процессах: машинное обучение, предиктивная аналитика, цифровые двойники, роботы, компьютерное зрение и многие другие. Новые технологические решения работают для непосвященного пользователя как черный ящик. При этом они несут с собой новые риски и вопросы, на которые необходимо найти ответы внутреннему аудиту для обеспечения надежности и эффективности системы внутреннего контроля организации. Насколько можно доверять результату работы нового технологического решения? Существует ли возможность с течением времени искажения работы технологии? Возможны ли ситуации, когда человек осознанно или неосознанно своими действиями может нарушить логику, изначально зашитую в работу технологического решения?
7. Еще одной областью внимания, которая особенно актуальна для российских организаций, является возможность поддержки внедренных технологий и программного обеспечения в долгосрочной перспективе. В период активного импортозамещения иностранного программного обеспечения организации не могли быстро нарастить компетенции собственной ИТ-команды, поэтому зачастую новое программное обеспечение продолжает поддерживаться разработчиком или сторонней организацией, оказывающей услуги ИТ-аутсорсинга. Важно проанализировать риски зависимости от ключевых поставщиков программного обеспечения в том случае, если они продолжают поддерживать продукт, или от ключевых сотрудников, которые являются носителями ключевых знаний об особенностях работы той или иной системы, и эти знания по различным причинам не были зафиксированы в технической документации.

Таким образом, цифровизация бизнес-процессов и системы внутреннего контроля привносит новые риски, выявляет новые области внимания и новые объекты аудита. Важно не просто полагаться на работу информационных систем, а на регулярной основе убеждаться в надежности и эффективности выстроенной вокруг цифровых решений системы внутреннего контроля. Важную роль в этом играет и комитет по аудиту, и руководство организации, и функция внутреннего аудита.

Члены комитета по аудиту должны держать в фокусе новые области риска и не упускать их из виду в ходе обсуждения тех или иных вопросов в повестке работы комитета. Руководству организации важно понимать, что нельзя слепо полагаться на работу технологических решений, и использовать внутренний аудит как инструмент проверки. Внутреннему аудиту важно наращивать компетенции для проверки новых рисков и объектов аудита, а также не бояться включать новые области в ежегодный план аудита с тем, чтобы убедиться в корректной работе системы внутреннего контроля или заблаговременно подсветить области, требующие улучшений.

Ознакомиться с презентацией

СКВОЗНАЯ ТРАНСФОРМАЦИЯ, ИЛИ КАК МЫ СВЯЗАЛИ АУДИТ, РИСКИ И КОНТРОЛЬ В ОДНУ АВТОМАТИЗИРОВАННУЮ СИСТЕМУ

Интеграция функций внутреннего аудита, внутреннего контроля и управления рисками позволяет компаниям формировать целостную систему управления рисками и повышать эффективность контрольной среды.

Т.С. МАКАРОВА
Директор по внутреннему аудиту и управлению рисками ООО «КЕХ ЕКОММЕРЦ» (Авито)

Аннотация

Статья описывает процесс сквозной трансформации функции аудита, управления рисками и внутреннего контроля в компании. В материале проанализированы недостатки прежней организационной модели (плоская структура, узкая сфера задач, риск конфликта интересов) и обоснованы преимущества новой структуры департамента, подчиненного напрямую генеральному директору: высокая независимость, прямой доступ к руководству, эффективная координация решений.

Ключевые слова: сквозная трансформация, аудит, управление рисками, внутренний контроль, комплаенс, автоматизированная система, организационная структура, формирование команды, подбор персонала, методологическая поддержка, внедрение технологий.

Коды JEL: M42, G32, M15, D23.

В Авито функция рисков и контроля существовала давно, но была представлена небольшой командой из семи человек с плоской структурой, подчинявшейся руководителю отдела в составе дирекции по закупкам.

Риски такой модели очевидны: потенциальная потеря независимости и конфликт интересов, возможное недоверие сотрудников и внешних заинтересованных сторон. Сфера задач была узкой – мелкие аудиты и описание процессов без комплексного подхода.

С приходом нового директора по аудиту и управлению рисками функция была переподчинена напрямую генеральному директору. Отдел был трансформирован в департамент, в котором выделено три направления: управление рисками, внутренний контроль (комплаенс) и внутренний аудит.

Для компании, не котирующейся на бирже, такое объединение под одним руководителем и подчинение генеральному директору – жизнеспособная модель. Преимущества новой структуры – высокая независимость, прямой доступ к руководству, эффективная координация решений и оперативная реакция на нарушения.

Жизнь не стоит на месте: весной 2024 года Авито получила от Банка России лицензию оператора финансовой платформы. Это направление регулируется законом № 211-ФЗ, и в существующий департамент функционально вошли риски и для этой платформы.

Формирование и развитие команды

Сформировать команду с нуля – это всегда особая задача.

Поскольку команда была совершенно новой, а люди пришли из разных бизнесов и индустрий, было критически важно не только притереться друг к другу, но и сразу задать правильные векторы развития. Была сделана ставка на работу с большими объемами данных, что естественно для ИТ-компании с ее множеством систем.

Основная цель – активно внедрять передовые технологии, чтобы повышать уровень уверенности (assurance) в результатах работы.

Сотрудники департамента много общаются с рынком: организуют референс-визиты, обмениваются опытом с коллегами. Внутри развита практика кросс-функциональных проектов, объединяя специалистов по контролю, рискам и аудиту. Это помогает команде сплотиться, а заодно создает здоровую взаимозаменяемость на случай изменений в команде.

Подбор разносторонней и профессиональной команды оказался непростой задачей. Изначально круг поиска ограничивался кандидатами с опытом в ИТ-сфере, а таких на рынке не так много. Кроме того, были нужны люди с особыми навыками – способные договариваться и выстраивать партнерские отношения, что не всегда характерно для специалистов из более жестких индустрий вроде производства или банков. Наконец, искали тех, кто горит желанием использовать новые технологии, а не просто работать по готовым гайдам.

Первый план работ был сформирован на основе статей финансовой отчетности, так как рисковой карты не было. Старались учитывать ограничения по ресурсам в период найма. Определили получателей отчетности – CEO и представителя акционера с квартальной периодичностью. Связали цели и метрики эффективности с индивидуальными картами сотрудников. Проводили стратегические сессии для выравнивания ожиданий команды, пришедшей из разных индустрий.

Внутренняя документация и автоматизация

Начали с политики внутреннего аудита, чтобы закрепить подотчетность. Затем разработали единую политику по системе управления рисками и внутреннего контроля (СУР и ВК), которая стала «зонтиком» и для регуляторных требований финансовой платформы, обеспечив единые подходы без противоречий.

Аудит, риски и контроль должны работать в одной системе. Карта рисков должна быть актуальной, формировать основу для описания контролей и для аудиторского плана. Наблюдения из аудитов, в свою очередь, должны возвращаться в карту рисков.

В компании есть единый провайдер (Security Vision Provider от GlowByte), продукт которого был сильно кастомизирован. В системе уже работают модули внутреннего контроля и аудита, активно развивается модуль рисков, что обеспечивает сквозной процесс и историчность данных.

В зрелых средах, где менеджеры осознанно подходят к работе и понимают влияние своих решений на смежные функции, централизованная функция риск-менеджмента может не быть необходимой. Как показали примеры «Яндекса» и Ozon, риски могут управляться децентрализовано самими владельцами процессов.

Подход руководителя внутреннего аудита и управления рисками – быть не «рисковиком» с формальными картами топ-10 рисков, а партнером для бизнеса. Важно не тормозить инициативы, а в момент запуска новых продуктов или фич аккуратно подсказывать, при необходимости привлекая нужных экспертов (юристов, финансистов, специалистов

по безопасности). Вторая важная роль – быть методологом, который помогает собрать целостную картину и связать между собой разные элементы системы управления рисками и контроля.

Вопрос цикличности аудита пока решается в формате коротких циклов. На первом этапе фокус на том, чтобы взять аудиты на год и обеспечить их последующий follow-up в следующем году. Главная задача сейчас – не набрать как можно больше проверок, а качественно закрыть уже выявленные рекомендации. Таким образом, аудиторский цикл составляет примерно год.

Трансформация – это всегда вызов, но именно он позволяет создавать эффективные и современные функции, действительно добавляющие ценность бизнесу.

Ознакомиться с презентацией

ТРАНСФОРМАЦИЯ ТЕХНОЛОГИЧЕСКОГО РИСК-МЕНЕДЖМЕНТА В ФИНАНСОВОЙ ИНФРАСТРУКТУРЕ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ

В современной технологической среде управление рисками уже невозможно рассматривать без учета технологических и киберрисков, а также рисков, связанных с использованием искусственного интеллекта.

С.В. ДЕМИДОВ
Заместитель Председателя Правления по информационной безопасности, Группа «Московская Биржа»

Аннотация

В статье рассматриваются современные подходы к управлению технологическими рисками в условиях цифровой трансформации экономики. Особое внимание уделяется киберрискам, рискам информационных технологий и рискам, связанным с использованием искусственного интеллекта. Анализируются ключевые вызовы, возникающие при внедрении новых технологий, а также роль функций внутреннего аудита и управления рисками в обеспечении устойчивости организаций в новой технологической реальности.

Ключевые слова: технологические риски; киберриски; информационные технологии; искусственный интеллект; управление рисками; внутренний аудит.

Коды JEL: M42, O33, G32, D81.

Группа «Московская Биржа» представляет собой уникальный финансовый институт, объединяющий две ключевые роли: инфраструктуру финансового рынка, и ИТ-компанию. Также группа активно развивает новые направления, включая цифровые финансовые активы (ЦФА) и маркетплейс «Финуслуги», торгово-информационный терминал «Трейд-Радар». Ежедневные объемы торгов на Московской Бирже превышают 1,4 трлн рублей, а в НРД хранятся активы на сумму более 60 трлн рублей.

Сложный современный мир часто описывается концепцией VUCA (Volatility, Uncertainty, Complexity, Ambiguity), характеризующей мир высокой неопределенности. В последние годы наблюдается тенденция к ее усугублению («VUCA в квадрате»). Современная экономика находится на перепутье: цифровая трансформация, усиление геополитической напряженности и стремительное развитие искусственного интеллекта (ИИ) кардинально трансформируют ландшафт нефинансовых рисков. Их объемы растут экспоненциально, создавая беспрецедентные вызовы для риск-менеджмента, особенно в сфере управления рисками **инфраструктуры финансового рынка**.

Для прогнозирования влияния ключевых тенденций на ландшафт рисков в ближайшие годы целесообразно анализировать их через призму четырех макрофакторов: социальные, политические, экономические и технологические тренды.

В 2026 году центральным элементом цифровой экосистемы становится взаимодействие с пользователем. В социальной среде доминирует тренд гиперперсонализации – индивидуализации предложений

на основе глубокого профилирования. Усложнение алгоритмов профилирования требует баланса между точностью предложений и соблюдением норм защиты данных.

Параллельно растет **гиперперсонализация мошенничества**. Рост фишинга с использованием технологий дипфейк и дипвойс, основанных на ИИ, приводит к массовым атакам на личные сбережения. Необходимость подтверждения целостности сеансов с пользователем становится критичной. Масштабные кампании дезинформации, спонсируемые как частными, так и государственными акторами, вызывают общественную панику, подрывают доверие к институтам и наносят серьезный репутационный ущерб.

Геополитическая нестабильность усиливает эту тенденцию. По данным Центрального банка, объем средств, потерянных гражданами РФ в результате мошенничества за 2025 год, составил более 29 млрд рублей. Государство усиливает регулирование информационной безопасности (законопроект «Антифрод 2.0», поправки в Уголовный кодекс). Банк России рассматривает возможность дисквалификации лиц, ответственных за информационную безопасность в случае реализации инфоугроз, приводящих к масштабным потерям. Это создает кадровый вызов: в условиях **угрозы уголовного и административного преследования** сфера информационной безопасности проигрывает в конкуренции с ИТ-индустрией за таланты.

Конкуренция с ИТ-сферой усугубляет кадровый голод в области информационной безопасности. Подготовка выпускников вузов зачастую запаздывает относительно развития технологий; дообучение специалистов занимает 1–1,5 года. Хотя Росстат заявляет о дефиците кадров на уровне 2% [3], ожидается, что приток на рынок будет состоять преимущественно из специалистов массовых профессий. **Битва за высокоэкспертные кадры продолжится**, но ее исход будет зависеть от способности организаций создавать привлекательные условия для работы в условиях высокой ответственности.

Также наблюдается тренд перехода экономики в режим работы 24/7, что требует больших инвестиций в надежность ИТ-инфраструктуры. В условиях замедления экономического роста такие инвестиции становятся все более сложными. Дополнительно осложняет ситуацию ограниченный объем российского технологического рынка и ограниченные возможности развития, продиктованные все той же экономической ситуацией. Возрастает потребность в гибких и адаптивных системах реагирования на внешние шоки.

Экономическая модель финансового сектора переходит к сервисной и платформенной парадигме. Компании меньше фокусируются на инвестициях в новые технологии, вендоры переходят на модели подписки. Развитие маркетплейсов и экосистем приводит к гиперсвязанности, бесшовности и непрерывному обновлению сервисов. Однако уязвимость одного партнера может вызвать каскадный сбой во всей системе. Риски третьих сторон кратно возрастают, требуя пересмотра подходов к управлению внешними зависимостями.

Технологические революции определяют будущее устойчивости и безопасности. Генеративный ИИ проникает во все бизнес-процессы – AI everywhere – от обслуживания клиентов и автоматизации отчетности до принятия операционных решений и управления рисками. Однако этот переход сопровождается ростом **рисков качества и безопасности**, особенно в условиях **hype-driven development** – когда технологии внедряются спешно, без должной проверки на надежность, этичность и устойчивость.

Переход от пилотных проектов к промышленной трансформации требует новых подходов к управлению рисками. Ранее риск ИИ относился к классическим операционным рискам, однако, руководствуясь консультативным докладом Банка России, целесообразно выделять риск ИИ в отдельный вид риска [4]. Это пересечение этических, комплаенс-рисков, операционных рисков и рисков информационной безопасности, требующее создания новых фреймворков управления.

В области киберрисков наблюдается дуализм: ИИ используется как для защиты, так и для нападения. Паритет смещен в пользу нападения – темпы развития сложности атак превышают темпы внедрения защитных решений. Это связано с зарегулированностью рынка средств защиты информации (сертификация ФСТЭК) и неограниченностью средств нападения. Порог входа в киберпреступность резко снижается: современный злоумышленник не обязан владеть сложными техническими навыками – достаточно использовать ИИ-инструменты и low-code-решения.

В условиях разнонаправленных трендов риск-менеджмент сталкивается с дилеммой: взять на себя ответственность за сложные риски или остаться черным ящиком – выполнять лишь базовую аналитику и формальную регистрацию событий. Приоритетной моделью становится роль риск-менеджера как энэйблера (enabler) – предоставление возможности бизнесу развиваться через управление риском. Выделены четыре фокуса трансформации риск-менеджмента:

1. **Работа с данными (Data Driven).** Данные становятся новым топливом в развитии организации. Риск-менеджмент перестает быть инструментом запретов – он становится гарантом качества данных и процессов их обработки. Необходима зрелая вторая линия защиты, способная управлять рисками, связанными с данными, их целостностью, происхождением и использованием.
2. **Работа с искусственным интеллектом.** Риски ИИ требуют отдельного фреймворка, объединяющего этические, регуляторные и киберриски. Пространство управления рисками ИИ трехмерно: необходимо оценивать защищенность системы, ее критичность для организации и покрытие контролями. Вовлечение риск-менеджмента необходимо на всех этапах жизненного цикла систем ИИ. В частности, в группе на 2026 год утверждены метрики риск-аппетита по риску ИИ, что демонстрирует готовность интегрировать новые технологии в критичные бизнес-процессы в рамках управляемой и контролируемой среды.
3. **Культура и люди.** Любая технология – это инструмент в руках человека. Фокус риск-менеджмента смещается с **формального соблюдения процедур** на создание **живой, адаптивной и ответственной культуры**. Каждый сотрудник – **активный участник защиты**. Наша стратегия развития СУР 4.0 (Система Управления Рисками), утвержденная в 2024 году на горизонт до 2028 года, делает риск-менеджмент полноценным участником развития бизнеса, внедряя риск-культуру в каждое подразделение.
4. **Кибермета**вселенная.** Организации не существуют в вакууме. В **кибермета**вселенной** – пространстве, где **физические, цифровые и виртуальные среды сливаются в единое целое,** – традиционные подходы к защите устаревают. Перед лицом новых, масштабных и персонализированных угроз необходимо использовать комплексный и многоуровневый подход к выстраиванию безопасности. Ключевая задача ИБ – обеспечение реализации бизнес-стратегии без снижения риск-защищенности и с соблюдением всех регуляторных обязательств, что обеспечит баланс между бизнесом, ИТ и ИБ. Наша стратегия информационной безопасности базируется на пяти столпах: ребалансировка (трансформация ландшафта ИБ в новой реальности), регулирование (помощь рынку во внедрении новых требований), культура (вовлечение индустрии), ИИ и инновации (развитие в управляемой среде), гибкость и мультитолерантность (адаптация ИБ под запросы бизнеса).

Способность риск-менеджмента быть гибким, выделять проблемные области, инвестировать ресурсы и создавать новые фреймворки является системным ответом на вызовы эпохи «VUCA в квадрате». Управление рисками должно эволюционировать от ограничительных мер к партнерству с бизнесом, обеспечивая безопасность в условиях возведенной в степень неопределенности. В этом контексте риск-менеджмент становится стратегическим драйвером устойчивого развития, способным превращать угрозы в возможности.

Список источников

1. Исследование Ассоциации ФинТех «3х10 трендов 2026 года».
2. Основные направления развития финансового рынка Российской Федерации на 2026 год и период 2027 и 2028 годов.
3. Основные направления развития финансового рынка Российской Федерации на 2025 год и период 2026 и 2027 годов.
4. Доклад для общественных консультаций «О подходах к регулированию деятельности финансовых инфлюенсеров».
5. Доклад для общественных консультаций «Применение искусственного интеллекта на финансовом рынке: текущий статус и условия дальнейшего развития».
6. Банк России. Информационное письмо о рисках, связанных с использованием технологий искусственного интеллекта.
7. Кодекс этики в сфере разработки и применения искусственного интеллекта на финансовом рынке.
8. Обзор операций, совершенных без добровольного согласия клиентов финансовых организаций.
9. ТАСС: ЦБ введет наказание для топ-менеджеров банков за слабую киберзащиту.
10. Интерфакс: Росстат сообщил о снижении безработицы в августе до 2,1%.

Ознакомиться с презентацией

ЗАКЛЮЧЕНИЕ

В условиях стремительных технологических изменений и усложнения бизнес-среды вопросы эффективного управления рисками, развития внутреннего аудита и совершенствования систем внутреннего контроля приобретают особое значение для устойчивости организаций.

Цифровая трансформация экономики формирует новые вызовы и одновременно открывает новые возможности для повышения эффективности контрольных функций. В этих условиях важную роль играет развитие современных методологических подходов, обмен профессиональным опытом и формирование компетенций, соответствующих новым требованиям цифровой среды.

Материалы настоящего выпуска отражают ключевые направления развития систем внутреннего аудита, внутреннего контроля и управления рисками и демонстрируют современные подходы к обеспечению устойчивости организаций.

Редакция надеется, что представленные материалы будут полезны специалистам в области внутреннего аудита, внутреннего контроля и управления рисками, членам советов директоров и комитетов по аудиту, руководителям организаций и всем, кто заинтересован в развитии эффективных систем корпоративного управления.

ГЛОССАРИЙ

Внутренний аудит – независимая и объективная деятельность по предоставлению гарантий и консультаций, направленная на совершенствование деятельности организации и повышение эффективности процессов управления рисками, внутреннего контроля и корпоративного управления.

Внутренний контроль – процесс, осуществляемый руководством и сотрудниками организации, направленный на обеспечение надежности финансовой отчетности, эффективности операций и соблюдения требований законодательства и внутренних регламентов.

Данные и управление данными – процессы обеспечения качества, целостности, доступности и надежности данных, используемых для принятия управленческих решений.

Карта рисков – инструмент визуализации и систематизации рисков организации, отражающий вероятность возникновения рисков и масштаб их потенциального воздействия.

Киберриски – риски, связанные с угрозами информационной безопасности, включая кибератаки, утечки данных и нарушение функционирования информационных систем.

Комитет по аудиту – комитет совета директоров, обеспечивающий контроль за финансовой отчетностью, системой внутреннего контроля, управлением рисками и деятельностью внутреннего и внешнего аудита.

Комитет по аудиту и рискам – специализированный комитет совета директоров, осуществляющий надзор за системой управления рисками, внутреннего контроля и внутреннего аудита.

Корпоративное управление – система взаимоотношений между советом директоров, исполнительным руководством и заинтересованными сторонами, направленная на эффективное управление организацией и защиту интересов собственников.

Риск-аппетит – уровень риска, который организация готова принять для достижения своих стратегических целей.

Система внутреннего контроля (СВК) – совокупность организационных мер, процедур и механизмов, направленных на обеспечение надежности и эффективности деятельности организации.

Система управления рисками (СУР) – совокупность процессов, методов и инструментов, обеспечивающих выявление, оценку, мониторинг и управление рисками организации.

Стратегический аудит – оценка стратегических решений и процессов стратегического управления организации с точки зрения их соответствия целям компании, уровню риск-аппетита и устойчивости бизнеса.

Технологические риски – риски, связанные с использованием информационных технологий, цифровых платформ и технологических решений в деятельности организации.

Третьи стороны (third-party risk) – риски, связанные с использованием внешних поставщиков услуг, партнеров и технологических провайдеров.

Управление модельными рисками – процессы выявления, оценки и контроля рисков, возникающих при использовании математических моделей, алгоритмов машинного обучения и систем искусственного интеллекта.

Цифровая трансформация – процесс внедрения цифровых технологий, изменяющий бизнес-процессы, модели управления и организационные структуры компаний.

Цифровая устойчивость – способность организации поддерживать непрерывность деятельности и устойчивость бизнес-процессов в условиях технологических изменений и киберугроз.

Цифровой аудит – применение цифровых технологий, анализа данных и автоматизированных инструментов для проведения аудиторских проверок.

СПИСОК СОКРАЩЕНИЙ

Общие аббревиатуры и термины

AI (Artificial Intelligence) – искусственный интеллект

CEO (Chief Executive Officer) – генеральный директор организации

d-people (data professionals) – специалисты, обладающие компетенциями в области анализа данных и цифровых технологий

GenAI (Generative Artificial Intelligence) – генеративный искусственный интеллект

HR (Human Resources) – управление персоналом

IT (Information Technology) – информационные технологии

KPI (Key Performance Indicators) – ключевые показатели эффективности

ML (Machine Learning) – машинное обучение

OKR (Objectives and Key Results) – система постановки целей и ключевых результатов

RACI (Responsible, Accountable, Consulted, Informed) – модель распределения ответственности

SQL (Structured Query Language) – язык структурированных запросов для управления базами данных

Сокращения в области корпоративного управления, аудита и контроля

ERM (Enterprise Risk Management) – система управления рисками организации

ВА – внутренний аудит

ВК – внутренний контроль

КАР – комитет по аудиту и рискам

СВА – служба внутреннего аудита

СВК – система внутреннего контроля

СД – совет директоров

СУР – система управления рисками

Международные организации и методологии

COBIT (Control Objectives for Information and Related Technologies) – международная методология управления и контроля информационных технологий

COSO (Committee of Sponsoring Organizations of the Treadway Commission) – организация, разработавшая международные концепции внутреннего контроля и управления рисками

COSO ERM (Enterprise Risk Management Framework) – концептуальная модель управления рисками организации

IIA (Institute of Internal Auditors) – международная профессиональная ассоциация внутренних аудиторов

NIST (National Institute of Standards and Technology) – Национальный институт стандартов и технологий США

NIST CSF (Cybersecurity Framework) – рамочная модель управления кибербезопасностью

Международные стандарты

IIA Global Internal Audit Standards – международные стандарты профессиональной практики внутреннего аудита

ISO (International Organization for Standardization) – Международная организация по стандартизации

ISO 31000 – международный стандарт управления рисками

ISO 37000 – международный стандарт корпоративного управления

ISO/IEC 27001 – международный стандарт системы менеджмента информационной безопасности

Экономическая классификация

JEL (Journal of Economic Literature Classification System) – международная система классификации научных исследований в области экономики