Банк России

МАТЕРИАЛЫ ЗАСЕДАНИЯ ЭКСПЕРТНОГО СОВЕТА ПО РЕГУЛИРОВАНИЮ, МЕТОДОЛОГИИ ВНУТРЕННЕГО АУДИТА, ВНУТРЕННЕГО КОНТРОЛЯ И УПРАВЛЕНИЯ РИСКАМИ В БАНКЕ РОССИИ И ФИНАНСОВЫХ ОРГАНИЗАЦИЯХ ОТ 18 ДЕКАБРЯ 2025 ГОДА

Москва
2025

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.

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 К ЧИТАТЕЛЯМ

Уважаемые коллеги!

Представляем итоги заседания Экспертного совета по регулированию, методологии внутреннего аудита, внутреннего контроля и управления рисками в Банке России и финансовых организациях, состоявшегося 18 декабря 2025 г. в Москве. Заседание прошло в очно-дистанционном формате и объединило представителей Банка России, финансовых организаций и компаний реального сектора, для которых качество рекомендаций внутреннего аудита и их практическая реализуемость остаются ключевым элементом эффективной системы корпоративного управления.

Отдельно стоит отметить, что состав участников Совета продолжает расширяться. В работе заседания все активнее принимают участие представители крупных промышленных, сырьевых, технологических компаний, цифровых и инфраструктурных институтов и культурных организаций, а также представители федеральных органов власти. В обсуждения вовлечены руководители и эксперты по внутреннему аудиту крупнейших российских компаний, в том числе из сфер телекоммуникаций и электроэнергетики. Расширение отраслевого охвата значительно повышает прикладную ценность дискуссий и позволяет рассматривать вопросы управления рисками и внутреннего контроля в многосекторной перспективе.

В центре обсуждения – новые вызовы, формирующие контуры современных систем управления: трансформация повестки комитетов по аудиту, развитие практик взаимодействия СВА[1] с менеджментом, изменение приоритетов управления рисками в условиях «устойчивой волатильности», совершенствование ВПОДК[2] с учетом операций с криптоактивами, а также правовые и технологические риски применения генеративного искусственного интеллекта. Особое внимание было уделено возможностям ответственного использования ИИ в управлении рисками, кибербезопасностью и защитой информации.

Докладчики представили результаты аналитических исследований, регуляторные новации и практические кейсы, демонстрирующие, как современные инструменты – от стресс-тестирования и интегрированной (единой) системы управления рисками до ИИ-агентов и экспертных систем – усиливают обоснованность управленческих решений при одновременном росте требований к контролю, качеству данных и ответственности.

---

1 Служба внутреннего аудита.

2 Внутренние процедуры оценки достаточности капитала.

Заседание прошло в формате открытого профессионального диалога. Обсуждались как стратегические аспекты: роль комитетов по аудиту, оптимальная архитектура трех линий защиты, учет новых рисков в ВПОДК, так и практические вопросы: настройка взаимодействия СВА и менеджмента, формирование культуры исполнения рекомендаций, развитие компетенций в области ИИ, кибербезопасности и работы с нефинансовой информацией.

Материалы, представленные в дайджесте, позволят по-новому взглянуть на взаимосвязь функции внутреннего аудита, риск-менеджмента, внутреннего контроля и цифровых технологий, укрепить системы управления рисками и внутреннего контроля, повысить эффективность работы комитетов по аудиту и тем самым внести значимый вклад в устойчивость российского финансового и нефинансового секторов и развитие современного 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

Экспертный совет по регулированию, методологии внутреннего аудита, внутреннего контроля и управления рисками в Банке России и финансовых организациях на заседании 18 декабря 2025 г. рассмотрел актуальные вопросы трансформации систем управления в условиях цифровизации, внедрения искусственного интеллекта, усложнения бизнес-моделей и роста требований к качеству внутреннего контроля и риск-менеджмента.

Основное внимание было уделено новым вызовам для комитетов по аудиту, эволюции практик взаимодействия СВА с менеджментом, изменению приоритетов CRO в условиях «устойчивой волатильности», развитию внутренних процедур оценки достаточности капитала с учетом операций с криптоактивами, а также правовым и технологическим рискам применения генеративного искусственного интеллекта при создании и использовании служебных РИД.

Участники Совета обсудили современные подходы к организации работы комитетов по аудиту в финансовом и нефинансовом секторах, практику формирования и согласования рекомендаций внутреннего аудита, методы повышения их качества, точности и реализуемости, механизмы взаимодействия трех линий защиты, а также вопросы готовности организаций к использованию ИИ в управлении рисками, кибербезопасностью и оценке качества систем защиты.

Были рассмотрены модели интеграции цифровых технологий в процессы контроля и мониторинга: применение стресс-сценариев и обратных стресс-тестов, использование процесс-майнинга, непрерывного мониторинга, технологий валидации моделей, а также ИИ-агентов и экспертных систем. Отдельное внимание уделено вопросам управления модельными рисками, снижению уязвимостей киберсреды и обеспечению качества данных.

Члены Совета подчеркнули, что современные функции внутреннего аудита и риск-менеджмента должны не только выявлять нарушения и недочеты, но и способствовать развитию бизнеса, повышению эффективности, устойчивости и технологической зрелости организаций. Были приведены примеры преобразования рекомендаций внутреннего аудита в полноценные управленческие решения, влияющие на архитектуру рисков, контрольные процедуры, кадровые процессы и технологические контуры.

Участники заседания также обсудили ключевые сложности: дефицит компетенций в области ИИ и кибербезопасности, необходимость усиления взаимодействия между линиями защиты, недостаточную автоматизацию процессов, требования к качеству данных, а также потребность в развитии новых механизмов корпоративного управления и интеграции нефинансовой информации.

По итогам обсуждения сделан вывод о необходимости дальнейшего развития подходов к работе комитетов по аудиту, расширения применения цифровых инструментов, совершенствования ВПОДК, внедрения риск-ориентированных технологий и формирования устойчивой среды для ответственного использования искусственного интеллекта.

Представленные материалы демонстрируют, что современные практики внутреннего аудита, риск-менеджмента и внутреннего контроля становятся важным элементом управления, влияющим на стратегическое развитие, устойчивость и конкурентоспособность организаций в условиях стремительной цифровой трансформации.

ТЕКУЩИЕ ВЫЗОВЫ И НЕКОТОРЫЕ ОСОБЕННОСТИ РАБОТЫ КОМИТЕТОВ ПО АУДИТУ В ФИНАНСОВОМ И НЕФИНАНСОВОМ СЕКТОРАХ

А.И. АРХАНГЕЛЬСКАЯ
Член Наблюдательного совета, независимый директор НКО НКЦ (АО)

А.А. САЛТЫКОВА
Независимый директор, член совета директоров компаний группы ОАО «РЖД»

Аннотация

В статье рассматриваются актуальные вызовы, с которыми сталкиваются советы директоров и комитеты по аудиту в условиях цифровизации, волатильности, усиления регуляторного давления и трансформации ожиданий заинтересованных сторон. Анализируются различия в повестке компаний финансового и нефинансового секторов, а также формирующиеся гибридные направления. Особое внимание уделено необходимости адаптации процессов, пересмотру моделей обеспечения уверенности, управлению модельными рисками, кибербезопасности и нефинансовой информации. Предложены стратегические и организационные меры, включающие интеграцию искусственного интеллекта (ИИ), гибкие формы и учитывающие международные практики. Подчеркивается растущая роль комитетов по аудиту в обеспечении устойчивости бизнеса и необходимость переосмысления их функций в контексте трансформации корпоративного управления.

Ключевые слова: корпоративное управление, комитет по аудиту, риск-менеджмент, искусственный интеллект, кибербезопасность, нефинансовая отчетность, стратегическая устойчивость.

Коды JEL: G34, M42, D81, O33, L2.

Повестка дня совета директоров охватывает вызовы и риски, характерные для компаний любых отраслей и обусловленные внешними условиями. Среди них – риск утраты стратегического фокуса и устойчивости бизнеса, вызовы технологического лидерства и экспертизы, кадровый дефицит и поколенческий сдвиг, рост требований к прозрачности и ответственности, а также инертность и стереотипность мышления.

При этом повестка имеет особенности в зависимости от сферы деятельности. Для компаний финансового сектора актуальны вопросы капитала и риск-метрик, регуляторные требования, контроль и операции в режиме реального времени, развитие открытых финансов. Для компаний нефинансового сектора – отраслевые требования, финансовая устойчивость, эффективность физических операций, цепочки поставок, продуктовый инжиниринг, снижение углеродного следа.

Параллельно формируются новые направления на стыке финансового и нефинансового секторов, обладающие смешанной проблематикой, – например, маркетплейсы физических товаров.

Каждый из бизнес-вызовов можно рассматривать как с точки зрения влияния на операционные и стратегические показатели, находящиеся в фокусе внимания менеджмента, так и с точки зрения аналитических метрик, влияющих на управление рисками и определение риск-аппетита – сферы ответственности комитетов по аудиту. Эти два взгляда интегрированы между собой.

Например, в контексте технологического сдвига актуальны вопросы использования облачной инфраструктуры, генеративного искусственного интеллекта, автоматизации и сокращения «технического долга». Эти технологии открывают возможности повышения продуктивности и эффективности, оптимизации затрат в средне- и долгосрочной перспективе. Однако в краткосрочной и среднесрочной перспективе они могут привести к росту операционных и капитальных затрат, а также повысить уязвимость организации.

С точки зрения управления ключевыми рисками и риск-аппетитом важно оценивать влияние этих факторов на такие аспекты, как time-to-market (время вывода продукта или услуги на рынок), cost-to-serve (совокупные затраты на обслуживание клиента или продукта), индекс лояльности клиентов и другие. Также необходимо учитывать влияние на киберустойчивость, технологическую независимость, импортозамещение и сохранность данных.

Большинство новых приоритетов совета директоров требует от комитетов по аудиту оперативной перенастройки процессов, компетенций, повестки и скорости принятия решений.

Использование искусственного интеллекта, расширение информационного обмена с третьими сторонами и стремительное технологическое развитие ставят перед организациями и комитетами по аудиту задачи совершенствования моделей обеспечения уверенности. Это включает развитие компетенций и трансформацию роли внутреннего аудита, новые акценты во взаимодействии с внешним аудитом, привлечение внешних экспертов в новом качестве, ведение диалога с регулятором, корректировку параметров оценки устойчивости и кибербезопасности.

Новые формы взаимодействия, включая технологические, требуют критического пересмотра требований к независимости и отсутствию конфликта интересов.

Приоритеты комитетов по аудиту расширяются не только за счет технологических аспектов и повышения скорости принятия решений, но и в связи с необходимостью ускоренного развития компетенций, преодоления когнитивных ловушек и решения кадровых проблем.

Особое внимание комитеты по аудиту уделяют надзорной деятельности, особенно в финансовом секторе. Важными направлениями здесь являются модельный риск (включая искусственный интеллект), противодействие отмыванию финансов, а также кредитные модели, регуляторные реформы, нормы операционной устойчивости.

С ростом нагрузки на комитет по аудиту целесообразно рассмотреть вопрос корректировки системы мотивации его членов.

Вызовы, стоящие перед советами директоров и комитетами по аудиту, требуют комплексных мер на нескольких уровнях.

Стратегические меры включают настройку и мониторинг показателей в отчетности для корректировки стратегии, проведение стресс-сценариев и «обратных стресс-тестов» (с выходом за пределы допустимых толерансов) на кратко- и среднесрочную перспективу, переход к многоальтернативному планированию, включая «взрывные сценарии», структурирование систем и процедур по COSO ICSR[3] и международным стандартам

[3] The Committee of Sponsoring Organizations` Supplemental Guidance ″Achieving Effective Internal Control over Sustainability Reporting″ – дополнительное руководство Комитета организаций-спонсоров «Обеспечение эффективного внутреннего контроля за отчетностью в области устойчивого развития».

внутреннего аудита (например, в части интегрированного заверения и стратегии внутреннего аудита), перераспределение ответственности между советом директоров, его комитетами и менеджментом, проведение тематических заседаний с углубленным анализом вопросов кибербезопасности, контрольной среды, искусственного интеллекта, цепочек поставок (для нефинансового сектора) и капитала (для финансового сектора).

С учетом растущей значимости нефинансовой информации и необходимости обеспечения уверенности в ее достоверности, в повестке комитетов по аудиту возникает вопрос о создании единой системы внутреннего контроля в отношении нефинансовой информации, обеспечении и постепенном повышении уровня уверенности, а также интеграции этой информации с финансовой отчетностью.

Организационные меры охватывают использование искусственного интеллекта для оптимизации рутинных задач, включение в состав комитетов специалистов по кибербезопасности, операционной устойчивости и модельному риску (для финансового сектора) или сотрудничество с ними как с постоянно приглашенными экспертами, приоритет гибких форм работы – совместные заседания комитетов, рабочие группы с участием членов разных комитетов, менеджмента и экспертов, участие членов комитета по аудиту в тематических заседаниях совета директоров, обучение, развитие командной работы, коммуникационных навыков, критического мышления и других компетенций.

Дополнительно стоит обратить внимание на возможности использования международного опыта (с учетом осмысления практики и критического анализа), например NIST[4] Cybersecurity Framework (CSF) 2.0, на развитие корпоративной ИИ-ответственности, внедрение метрик для новых и критически важных областей (например, доля высокорискованных систем с полной валидацией), специальные процедуры для облачных структур и работы с третьими сторонами – риски концентрации, право на аудит, получение логов, меры при прекращении использования облака и другие.

Ожидания стейкхолдеров от деятельности советов директоров и комитетов по аудиту постоянно растут. Это касается компетенций, скорости и качества решений, уровня вовлеченности и требует от членов комитетов увеличения временных инвестиций.

С учетом текущей динамики компетенции в области управления рисками и контроля остаются приоритетными для комитетов по аудиту и продолжают расширяться. Особенно быстро растет ответственность в отношении нефинансовой информации, для которой уже сейчас необходимы новые модели обеспечения уверенности. Принцип «системы аудируют системы» будет применяться как к финансовой, так и к нефинансовой информации.

Будущее комитетов во многом зависит от четкого понимания обозначенных вызовов и институционального ответа на него – трансформации корпоративного управления: перехода от фиксированных комитетов к гибким рабочим группам с участием директоров, интеграции искусственного интеллекта в корпоративное управление, включая возможности использования ИИ-систем в корпоративном управлении и его оценке, быстрого наращивания компетенций в новых областях, а также других нетипичных для сложившейся практики инструментов.

[4] The National Institute of Standards and Technology, USA – Национальный институт стандартов и технологий, США.

Список литературы

1. 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».
2. Кибербезопасность. Руководство по применению тематических требований. Международные основы профессиональной практики внутреннего аудита. URL: https://www.theiia.org/globalassets/site/standards/topical-requirements/cybersecurity/cybersecurity_tr_user_guide_russian.pdf. Дата обращения: 12.09.2025.
3. Кибербезопасность. Тематические требования. Международные основы профессиональной практики внутреннего аудита. URL: https://www.theiia.org/globalassets/site/standards/topical-requirements/cybersecurity/cybersecurity_topical_requirement_russian. pdf. Дата обращения: 12.09.2025.
4. Международные стандарты внутреннего аудита. URL: https://www.iia-ru.ru/upload/inner-auditor/articles/2023-7726%20GUI%20Global%20IA%20Standards-Russian. pdf. Дата обращения: 12.09.2025.
5. Национальный доклад по корпоративному управлению. Выпуск XIV. Национальный совет по корпоративному управлению. 2025. URL: https://nccg.ru/assets/files/ndku/v14/nacionalnyj-doklad-po-korporativnomu-upravleniyu-2025-3-17. pdf. Дата обращения: 12.09.2025.
6. Обзор практик корпоративного управления. Портрет совета директоров. Аналитическое исследование НОКС. 2024. URL: https://nokc.org.ru/wp-content/uploads/2025/02/portrait-bod-2024. pdf. Дата обращения: 12.09.2025.
7. Письмо Банка России от 10.04.2014 № 06-52/2463 «О Кодексе корпоративного управления».
8. Письмо Банка России от 15.09.2016 № ИН-015-52/66 «О положениях о совете директоров и о комитетах совета директоров публичного акционерного общества».
9. Corporate Governance Review 2024. URL: https://www.independentdirectorsdatabank.in/img/newsletter/2025/6784ca5d68 644. pdf. Дата обращения: 12.09.2025.
10. Gartner Top Strategic Technology Trends for 2026. URL: https://www.gartner.com/en/articles/top-technology-trends-2026. Дата обращения: 24.10.2025.
11. Global Risk in Focus 2025. URL: https://www.theiia.org/globalassets/site/foundation/latest-research-and-products/risk-in-focus/2025/2025-global-report-en-riskinfocus. pdf. Дата обращения: 12.09.2025.
12. The Committee of Sponsoring Organizations` Fraud Risk Management Guide. URL: https://www.coso.org/frauddeterrence. Дата обращения: 12.09.2025.
13. The Committee of Sponsoring Organizations` Guidance on Enterprise Risk Management. URL: https://www.coso.org/guidance-erm. Дата обращения: 12.09.2025.
14. The Committee of Sponsoring Organizations` Guidance on Internal Control. URL: https://www.coso.org/guidance-on-ic. Дата обращения: 12.09.2025.
15. The NIST Cybersecurity Framework (CSF) 2.0. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP. 29. pdf. Дата обращения: 12.09.2025.

Ознакомиться с презентацией

ПРАКТИКА ВЗАИМОДЕЙСТВИЯ СВА В ПРОЦЕССЕ ПОДГОТОВКИ И РЕАЛИЗАЦИИ РЕКОМЕНДАЦИЙ ВНУТРЕННЕГО АУДИТА

Я.С. ЛИМАН
Руководитель Службы внутреннего аудита АО РНПК

Аннотация

Для АО РНПК, как и для большинства компаний на финансовом рынке, формирование и становление практики взаимодействия Службы внутреннего аудита с высшим исполнительным руководством, операционным руководством, владельцами бизнес-процессов, в том числе в рамках разработки, согласования и исполнения планов мероприятий соответственно рекомендациям СВА, полученным в ходе проверок, – это обязательный и значимый этап реализации эффективного внутреннего аудита. Данный вопрос является комплексным и для отдельных компаний – сложным, что может приводить к неисполнению либо затягиванию сроков исполнения рекомендаций внутреннего аудита. В статье приведен опыт выстраивания конструктивных отношений и эффективных коммуникаций. Выделены основные зоны, требующие внимания. Подчеркнута важность открытости СВА и неформального взаимодействия с сотрудниками организации на постоянной основе, что позволяет сотрудникам не бояться, а видеть в сотрудниках СВА союзников, стремящихся повысить эффективность и помочь своевременно управлять возникающими в ходе деятельности рисками. Схематично рассмотрены варианты взаимодействия СВА на разных этапах зрелости и масштабах бизнеса компании.

Ключевые слова: внутренний аудит, эффективная коммуникация, рекомендации и планы мероприятий, мониторинг планов мероприятий.

Коды JEL: G22, G30, M14.

Формирование и становление практики взаимодействия СВА с высшим исполнительным руководством, операционным руководством, владельцами бизнес-процессов при разработке ими плана мероприятий по рекомендациям, полученным по итогам проверки, является обязательным и значимым этапом реализации эффективного внутреннего аудита. Ключевым звеном является умение руководителя СВА сформировать доверительную атмосферу и позитивное отношение к внутреннему аудиту, в том числе путем акцентирования внимания менеджмента на преимуществах, которые возникают в ходе деятельности СВА, включая рекомендации по итогам проверок и консультации в качестве независимого бизнес-партнера.

В АО РНПК такое развитие и выстраивание отношений происходило постепенно. На первоначальном этапе руководителем СВА уделялось значительное время развитию как формальных, так и неформальных коммуникаций в целях установления взаимопонимания в следующих вопросах:

- стратегические цели и интересы;
- регуляторные требования;
- бизнес-процессы и взаимодействие подразделений;
- выявление, оценка и управление рисками;
- препятствия и проблемы в деятельности;
- подготовка финансовой и регуляторной отчетности.

Постепенно между высшим исполнительным руководством и СВА появилось взаимопонимание в вопросах приоритетов в области управления рисками, повышения корпоративной культуры, построения эффективной системы внутреннего контроля с усилением второй линии защиты (выделение СКиВК) и повышения способности адаптации к изменениям.

Руководитель СВА стала максимально вовлеченной в коммуникационный процесс с правом присутствия на заседаниях комитетов Наблюдательного совета, Правления, комитетов Общества, ключевых совещаниях высшего и исполнительного руководства и так далее. Кроме того, проведение в течение года отдельных встреч руководителя СВА с руководителями высшего звена и членами Наблюдательного совета дало возможность выстроить конструктивные и ясные отношения, узнать их точки зрения, чаяния и опасения. Также на постоянной основе встречи проводятся с владельцами бизнес-процессов и ключевыми представителями операционного руководства, в том числе с целью актуализации бизнес-целей и процессов под влиянием динамично меняющейся внешней среды на российском страховом рынке.

Для всестороннего понимания порядка взаимодействия в компании и особенностей ее контрольной среды дополнительное внимание руководитель СВА уделяет созданию возможностей неформального взаимодействия с сотрудниками организации на постоянной основе. Таким образом удается достичь открытого общения и уважения со стороны как руководящего звена, так и рядовых сотрудников компании. Такая открытость СВА позволяет видеть в сотрудниках СВА союзников, стремящихся повысить эффективность и помочь своевременно управлять возникающими в ходе деятельности рисками.

Рекомендации, выданные СВА в ходе проверки, в обязательном порядке должны быть вынесены на обсуждение в момент представления отчета владельцу бизнес-процесса и (или) иному руководителю. В практике нашей компании они также рассматриваются на заседании Правления.

Согласно международным стандартам внутреннего аудита, СВА осуществляет мониторинг выполнения руководством плана мероприятий и продолжает в целях подтверждения исполнения плана обмениваться информацией с владельцем бизнес-процесса и (или) руководством объекта аудита.

Для эффективного взаимодействия в процессе разработки и согласования плана мероприятий по рекомендациям, выданным СВА в ходе проверки бизнес-процесса, следует четким образом определить распределение ответственности между участниками мониторинговой активности (СВА и владельцем бизнес-процесса и (или) руководством объекта аудита).

Например, на первоначальном этапе может быть установлено следующее:

- мероприятия по выданным СВА по итогам проверки рекомендациям разрабатываются владельцами бизнес-процессов;
- СВА может внести свое видение формулировок, сроков и ответственных исполнителей;
- по одному аудиторскому наблюдению может быть разработано несколько корректирующих действий;
- планы мероприятий согласовываются по электронной почте и утверждаются генеральным директором (на бумажном носителе);
- в случае принципиальных разногласий между СВА и владельцем бизнес-процесса / руководством обе стороны должны иметь возможность выразить и аргументировать свои позиции и запустить процедуру урегулирования разногласий (например, вынести вопрос на заседание высшего исполнительного руководства или заседание Комитета по аудиту).

По мере роста корпоративной культуры, а также зрелости и развития практики взаимодействия СВА в процессе мониторинга исполнения рекомендаций по итогам проверки может быть реализован порядок, характеризующийся следующими критериями:

- СВА: приоритизация мероприятий, поручение владельцу бизнес-процесса составление плана мероприятий, организация встреч с руководством/сотрудниками аудируемых подразделений и так далее;
- разработка владельцами бизнес-процессов планов мероприятий по рекомендациям, выданным СВА по итогам проверки;
- согласование плана мероприятий владельцем бизнес-процесса, менеджментом, руководителем СВА и утверждение президентом в рамках автоматизированного процесса в ПО;
- рассылка задач на исполнение в системе автоматического документооборота;
- еженедельный мониторинг сотрудниками СВА хода исполнения мероприятий планов в ПО;
- проведение руководителем СВА промежуточных статусов/совещаний по ходу реализации планов по приоритетным бизнес-процессам;
- срок исполнения / ответственный за мероприятие плана, утвержденного президентом, не может быть изменен по согласованию с СВА;
- изменения в план могут быть внесены только по итогам встречи с президентом и руководителем СВА при представлении исполнителем весомого объяснения причин невозможности/неактуальности мероприятия;
- ежеквартальное представление итогов мониторинга Комитету по аудиту.

Для подтверждения исполнения ответственными сотрудниками мероприятий плана СВА использует следующие инструменты:

- направление запросов о ходе выполнения мероприятий;
- проведение последующих оценок в соответствии с риск-ориентированным подходом;
- еженедельная актуализация статусов мероприятий в ходе мониторинга.

При резком расширении бизнеса, вызванном изменением внешней геополитической среды и регуляторных условий функционирования, и соответствующем быстром и значительном росте численности персонала компания столкнулась с необычным риском: новые сотрудники приходили из компаний с более слабой корпоративной культурой и зачастую не знали и (или) не имели опыта понимания роли СВА как бизнес-партнера и консультанта исполнительных органов общества, напрямую подотчетного Комитету по аудиту и Наблюдательному совету.

В такой ситуации возникла угроза следующих негативных последствий:

- несвоевременное исполнение рекомендаций СВА;
- неконструктивный диалог с сотрудниками СВА;
- низкая вовлеченность в эффективное взаимодействие с сотрудниками СВА.

СВА предприняла дополнительные действия, направленные на снижение возникших угроз. Например:

- участие руководителя СВА в адаптационных встречах для новых сотрудников общества;
- проведение встреч с СВА для сотрудников общества;
- разъяснения для Руководителей направлений деятельности компании и операционных подразделений.

Данные мероприятия привели к положительному результату – восстановлению ясности понимания сотрудниками роли и значимости СВА.

Список литературы

1. Международные стандарты внутреннего аудита (The Institute of Internal Auditors – Международный институт внутренних аудиторов, 2024).

Ознакомиться с презентацией

М.Ю. ЦИБУЛЕВСКИЙ
Партнер, руководитель группы по оказанию услуг для организаций финансового сектора ООО «Б1 – Консалт»

ИССЛЕДОВАНИЕ МНЕНИЙ РУКОВОДИТЕЛЕЙ ПО РИСКАМ (CRO) РОССИЙСКИХ БАНКОВ

Аннотация

Современный российский банковский сектор функционирует в условиях «устойчивой волатильности», характеризующейся сложным переплетением геополитических сдвигов, макроэкономической нестабильности, стремительной технологической эволюции и трансформации потребительского поведения. Настоящее исследование анализирует ожидания банков в области оценки рисков и управления ими на системном уровне. Обсуждается необходимость управления традиционными рисками в изменившихся условиях, а также адекватная оценка новых угроз. Это первое столь масштабное исследование, посвященное исключительно взглядам и приоритетам руководителей служб управления рисками на российском рынке, которое закладывает основу для ежегодного мониторинга трендов в управлении рисками.

Ключевые слова: управление рисками, интегрированный риск-менеджмент, операционные риски, кредитные риски, нефинансовые риски, искусственный интеллект.

Коды JEL: D81, G20, G32.

Современный этап развития российского банковского сектора характеризуется фундаментальными трансформациями, формирующими уникальные условия ведения бизнеса, которые можно характеризовать как состояние «устойчивой волатильности». Это сочетание постоянной неопределенности, вызванной внешними и внутренними шоками, и способности финансовой системы к сопротивлению этим вызовам. Главной задачей для банков является не только преодоление кризисов, но и обеспечение устойчивого развития в условиях нестабильности, которая становится нормой.

Целями настоящего исследования являются анализ и сопоставление ожиданий банков в области оценки рисков и управления ими на системном уровне, выявление ключевых вызовов и возможностей в повестке руководителей служб управления рисками (CRO, Chief Risk Officers). В основе исследования лежат мнения 24 кредитных организаций разного масштаба, совокупно представляющих 78% активов банковского сектора России. Это первое столь масштабное исследование, посвященное исключительно взглядам CRO и их приоритетам на российском рынке, которое закладывает основу для ежегодного мониторинга трендов в управлении рисками. Для сравнения с общемировой практикой используются результаты аналогичного опроса группы EY и Института международных финансов (Institute of International Finance) за 2025 г., охватывающего 115 банков в 45 странах.

Внешнеполитическая напряженность и макроэкономическая нестабильность продолжают в значительной мере определять повестку. Основными рисками в приоритете на ближайший год для российских CRO являются кредитный риск, процентный риск банковской книги, риск ликвидности и фондирования, кредитный риск контрагента, а также риски ИБ и риски ИС. Их зарубежные коллеги значительно чаще фокусируются на рисках ИБ, а также выделяют комплексную категорию – «геополитический риск». Приоритетными направлениями развития являются инструменты оценки рисков, данные и отчетность, риск-аппетит, системы и инструменты раннего предупреждения, а также внедрение и модернизация обеспечивающих ИТ-решений. Кроме того, CRO российских банков уделяют большое внимание стандартизации и улучшению модельной документации, внедрению ИИ в систему управления рисками, а также управлению риском концентрации, в том числе в связи с внедрением норматива Н30 для СЗКО и оптимизации норматива достаточности капитала.

Обеспечение качества данных является ключевым драйвером эффективности управления риском. Подавляющее большинство (58%) опрошенных банков оценивают уровень зрелости управления качеством данных в своем риск-менеджменте как средний, одна пятая (21%) – как низкий. Значимым фактором является выделение роли ответственного лица по данным, зачастую на уровне директора (chief data officer, CDO). Это характерно в первую очередь для СКЗО (89% опрошенных). В банках следующей размерной категории – не являющихся СЗКО, но имеющих величину активов свыше 500 млрд руб., – задачи управления данными обычно (75% опрошенных) возложены на ИТ-подразделение, в то время как более половины (64%) опрошенных мелких банков возложили функции CDO на CRO.

Технологии искусственного интеллекта (ИИ), включая генеративный искусственный интеллект (GenAI), имеют значительные перспективы применения в управлении рисками, что обосновывает активное внедрение ИИ банками. Основными направлениями, в которых российские банки внедряют ИИ, являются обработка жалоб и обращений клиентов (42%), а также выявление мошенничества (38%), кредитный скоринг (38%) и оценка рисков (38%). Зарубежные банки демонстрируют сравнимый прогресс по внедрению ИИ в кредитном скоринге (40%), но при этом доли банков, внедривших ИИ в выявлении мошенничества, финансовом мониторинге, валидации моделей и выявлении источников риска информационной безопасности, примерно вдвое больше. Российские CRO рассматривают указанные направления как перспективные на горизонте 5 лет, дополнительно выделяя использование инструментов ИИ в обучении сотрудников в области риск-менеджмента и управления данными.

Однако при этом вложения российских банков в ИИ остаются ограниченными. 52% опрошенных российских банков не выделяют на развитие ИИ в управлении рисками отдельный бюджет; 24% выделяют менее 500 млн руб. в год. 41% опрошенных CRO зарубежных банков также отмечают бюджетирование как ограничение при внедрении ИИ в управлении рисками.

При этом применение ИИ банками является источником дополнительных рисков, которые требуют разработки и внедрения соответствующих инструментов для управления ими. Среди опрошенных российских банков 54% анализируют риски ИИ, 33% на момент опроса только планировали их анализировать. Среди банков существует расхождение в том, следует ли выделять риск ИИ как отдельный вид риска в таксономии или включать его в другие виды рисков. На продвинутом уровне развития – с сформированным подходом и утвержденной методологией управления рисками ИИ – находится 8% опрошенных банков.

Быстрое развитие новых технологий приводит к изменению набора профессиональных навыков риск-менеджеров. На горизонте 5 лет CRO ожидают падения значимости компетенций в управлении финансовыми рисками (кредитный, рыночный риски и риск ликвидности)

и интегрированном риск-менеджменте, а также роста значимости навыков в области ИИ и машинного обучения, управления качеством данных, операционной устойчивости, и обеспечении непрерывности и восстановления деятельности. Актуальными останутся познания в области кибербезопасности.

Отдельным актуальным для российского рынка направлением является развитие регулирования в области нормативов достаточности капитала, в частности обязательный переход СЗКО на подход на основе внутренних рейтингов (ПВР, Положение Банка России № 744-П) для оценки кредитного риска и расчетный коэффициент внутренних потерь (КВП, положения Банка России № 744-П и № 814-П) для оценки операционного риска. 17% опрошенных банков применяют ПВР, еще 37% планируют перейти на него в ближайшие 1–5 лет; для расчетного КВП указанные величины составляют 17 и 25% соответственно. При этом среди планирующих переход на ПВР 24% опрошенных ожидают роста величины оценки кредитного риска (что для них является отрицательным эффектом), 35% считают, что положительный эффект будет только в краткосрочной перспективе, а 6% не ожидают эффекта. Переход на ПВР – сложный с регуляторной точки зрения и трудоемкий процесс; практически все банки выделяют сложности с ретроспективным обновлением данных (94%), ужесточенными требованиями к валидации моделей (82%,) необходимостью усиления контроля качества данных (71%) и разработкой дополнительных внутренних нормативных документов (71%).

Список литературы

1. Положение Банка России от 07.12.2020 №744-П «О порядке расчета размера операционного риска («Базель III») и осуществления Банком России надзора за его соблюдением».
2. Положение Банка России от 30.01.2023 № 814-П «О порядке расчета размера операционного риска банковской группы».
3. Положение Банка России от 02.11.2024 № 845-П «О порядке расчета величины кредитного риска банками с применением банковских методик управления кредитным риском и моделей количественной оценки кредитного риска».
4. Устойчивая волатильность: балансируя между вызовами и возможностями – исследование мнений CRO: тренды в управлении банковскими рисками. URL: https://b1. ru/upload/sprint. editor/cda/mobxglvm7px59hukriy8ynfr9r4fttym/b1-cro-survey-trends-in-banking-risk-management. pdf. Дата обращения: 25.09.2025.
5. Agility in volatility: Rebalancing CRO priorities in a shifting risk matrix – 14th annual EY/IIF global bank risk management survey. URL: https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gl/insights/banking-capital-markets/documents/ey-and-institute-of-international-finance-bank-risk-management-survey-02–2025. pdf. Дата обращения: 25.09.2025.

Ознакомиться с презентацией

С.В. ЗУБКОВА
Кандидат экономических наук, доцент кафедры банковского дела и монетарного регулирования Финансового факультета Финансового университета при Правительстве Российской Федерации

НОВЫЕ РИСКИ И РАЗВИТИЕ ВПОДК В БАНКОВСКОМ СЕКТОРЕ

Аннотация

В статье рассматриваются актуальные вопросы развития внутренних процедур оценки достаточности капитала кредитных организаций, а также рассматривается необходимость совершенствования пруденциального регулирования в России с учетом быстрого расширения операций с криптоактивами в мире.

Ключевые слова: ВПОДК, банки, криптоактивы, технологии распределенного реестра, токенизированные активы, банковские риски.

Коды JEL: G21, G28, G32, G38, E58, G12, O33, K22, K24, F65.

Базельский комитет по банковскому надзору согласовал Базель III в качестве глобального стандарта для требований к капиталу банков и их надзора еще в 2010 году. Некоторые страны, включая Россию, приступили практически сразу к его реализации. Однако достаточно быстро стало понятно, что данные рекомендации требуют работы по их совершенствованию, которая завершилась только в 2017 году.

Необходимо отметить, что многие страны до сих пор не внедрили рекомендации из первоначального варианта. Например, ЕС выбрал длительный переход до 2032 г., в течение которого будут действовать мягкие переходные корректировки, в первую очередь коэффициентов взвешивания по риску некоторых активов.

Ведущие американские банковские регуляторы – Федеральная резервная система, Федеральная корпорация страхования депозитов (FDIC) и Управление контролера денежного обращения (OCC) в июле 2023 г. предложили реформу регулирования, которая направлена на ужесточение требований к капиталу и снижение их зависимости от собственных оценок банков. По оценкам FDIC, предложение «Завершение игры» 2023 г. увеличило бы требования к капиталу для системно значимых банков США примерно на 100%, что значительно больше, чем в ЕС.

США предложили практически полностью отказаться от использования подхода, основанного на внутренних рейтингах (IRB), для оценки кредитного риска, так что даже крупнейшим банкам пришлось бы прибегнуть к стандартизированному подходу (RSA) для оценки кредитного риска (пересмотренный Базель II), который не только менее чувствителен к риску, но и в среднем все еще приводит к несколько более высоким требованиям к капиталу. Обсуждение подходов к внедрению рекомендаций БКБН в США еще не завершено. Изменившийся политический климат и различные проблемы говорят о переносе сроков и способов внедрения Базеля III в США на период далее 2026 года.

Особое внимание в свете внедрения Базельских рекомендаций приобретают стандарты для международных банков по пруденциальному подходу к рискам, связанным с операциями кредитных организаций с криптоактивами. Эти стандарты планируется внедрить к 1 января 2027 года.

Европейский банк провел в 2023 г. исследование цифровой трансформации европейских банков. В результате было выявлено, что большинство банков начали разрабатывать свои стратегии цифровой трансформации лишь в последние годы, ориентируясь на показатели выручки и сокращения затрат. При этом особое внимание практически все банки уделяют внедрению технологий, которые способствуют их цифровой трансформации. Большинство банков отметили интерес к внедрению технологий распределенного реестра, при этом Европейский банк отметил, что операции банков с криптоактивами не несут пока значительных рисков ввиду их малой доли в основном бизнесе банков.

В то же время анализ последних данных показывает, что операции с криптоактивами активно растут. Так, рыночная капитализация криптоактивов выросла до 4,2 трлн долларов США в III квартале 2025 г. (3,9 трлн долларов США, декабрь 2024 г.), рыночная капитализация стейблкойнов выросла на 14% с конца II квартала, превысив 300 млрд долларов США.

Использование стейблкойнов в трансграничных транзакциях растет по сравнению с другими криптоактивами. Дальнейшее расширение зависит от их использования для платежей, в том числе за пределами их криптопространства, денежных переводов и трансграничных потоков. В целом рынки ожидают быстрого роста внедрения стейблкойнов в ближайшем будущем, хотя и в условиях широкой неопределенности.

Большинство банков как в России, так и в мире воздерживаются от криптоактивов, в то время как некоторые изучают возможности использования технологии распределенного реестра (DLT) для повышения эффективности, снижения затрат и предложения новых услуг клиентам.

Тем не менее этот сектор требует постоянного тщательного мониторинга, поскольку криптоактивы динамичны, и связи с более широким финансовым сектором в будущем могут значительно возрасти. Риски могут увеличиться по мере дальнейшего развития и большей ясности экосистемы криптоактивов (например, постторговых услуг).

Возможные будущие операции банков с криптоактивами – прямо или косвенно – приведут к значительным рискам, не охватываемым действующими пруденциальными нормами. Это риски не только в части инвестиций в криптоактивы, но и риски кредитования деятельности, связанной с криптоактивами, партнерства с технологическими компаниями в области токенизации активов и депозитов и другие. Консервативная глобальная минимальная пруденциальная система жизненно важна для защиты банковской системы от этих рисков.

Система ВПОДК, включающая оценку рисков, связанных с криптоактивами, должна включать такие аспекты, как:

- выявление рисков: оценка специфических рисков криптоактивов (ценовых, ликвидных, операционных, рисков соответствия, киберрисков и так далее);
- измерение и взвешивание: определение подверженности риску и применение соответствующих весовых коэффициентов риска в соответствии с пруденциальными рекомендациями;
- стрессовые сценарии: разработка стрессовых сценариев, специфичных для криптоактивов (например, обвал цен, проблемы с хранением);
- выделенный капитал: определение дополнительного капитала, необходимого для покрытия этих рисков, путем интеграции этих воздействий в общие расчеты ВПОДК;
- управление: разработка четкой политики приобретения, хранения и управления криптоактивами.

Завершение разработки стандарта Базельского комитета по банковскому надзору (БКБН) по пруденциальному подходу к банковским рискам, связанным с криптоактивами, – важный шаг в этом отношении.

Стандарт обеспечивает согласованный международный подход к регулированию и надзору в отношении банковских рисков, связанных с криптоактивами, и направлен на достижение баланса между ответственными инновациями частного сектора и эффективным управлением банковскими рисками и финансовой стабильностью.

С точки зрения Европейского союза, стандарт БКБН дополняет предстоящее регулирование сектора криптоактивов посредством регулирования рынков криптоактивов.

БКБН разделил криптоактивы на две группы. К токенизированным традиционным активам и стейблкойнам с эффективными механизмами стабилизации, соответствующим условиям классификации, будут применяться те же требования к собственным средствам, что и к их резервным активам или активам, на которые они ссылаются, с возможностью для надзорных органов вводить дополнительные требования. Данный аспект уже учитывается в только что вступивших в действие инструкциях Банка России № 220-И и 221-И.

Вторая группа, включающая наиболее рискованные формы криптоактивов, должна иметь весовой коэффициент риска 1250%, если только они не соответствуют определенным критериям признания хеджирования; в этом случае к ним должны применяться правила оценки рыночного риска. Лимиты удержания также будут применяться к второй группе активов. Банки также обязаны проводить комплексную проверку (due diligence), чтобы убедиться в наличии у них адекватного понимания механизмов стабилизации стейблкойнов, с которыми они сталкиваются, а также эффективности этих механизмов. В рамках комплексной проверки банки обязаны проводить статистические или иные тесты, демонстрирующие, что стейблкойн сохраняет стабильность по сравнению с референтным активом. Базельский комитет в июле 2024 г. опубликовал свои рекомендации по раскрытию информации, связанной с банковскими рисками в отношении криптоактивов, которые включают стандартизированную таблицу раскрытия информации и набор шаблонов для банковских рисков в отношении криптоактивов. Ожидается, что банки будут ежегодно раскрывать качественную информацию о своей деятельности, связанной с криптоактивами, и подходе, используемом при оценке условий классификации.

Для российских банков данный стандарт пока не является актуальным, так как законодательно не приняты нормативные акты, которые бы полностью систематизировали операции с криптоактивами. Однако существенные темпы роста операций с криптоактивами, которые могут демонстрировать сильную волатильность, требуют активизации нормотворческой работы в этой области.

В России необходима долгосрочная система пруденциального регулирования для криптоактивов и связанной с ними деятельности.

Новый проект указания «О требованиях к системе управления рисками и капиталом в кредитных организациях, в банковских группах», разработанный Банком России, планируется ввести в действие в 2026 году. Однако представляется, что в данном проекте должны появиться статьи, посвященные оценке рисков банковской деятельности с криптоактивами.

В своих системах оценки достаточности капитала банки должны предусмотреть:

- проведение всесторонней проверки и оценки рисков, прежде чем приступать к деятельности, связанной с криптоактивами, а также убедиться, что они понимают и принимают меры по снижению любых рисков, которые они могут принять при этом;
- при привлечении третьей стороны для осуществления деятельности, связанной с криптоактивами, необходим учет принципов и требований к банковскому аутсорсингу;
- применение надежных механизмов контроля за рисками, предусматривающих четкую подотчетность и предоставление совету директоров соответствующей отчетности по ключевым рискам, связанным с новым видом деятельности и предприятиями.

В заключение необходимо отметить, что развитие пруденциального регулирования в сфере банковских операций с криптоактивами, в том числе развитие ВПОДК с учетом рассмотренного выше Базельского стандарта, позволит поддерживать не только финансовую устойчивость и стабильность отдельных кредитных организаций, но и обеспечить монетарный цифровой суверенитет страны в целом.

Список литературы

1. Гюнтер И.Н., Фейзрахманова Н.М., Дахова З.И. Токенизированные безналичные деньги в банках // Научный результат. Экономические исследования. 2024. Т. 10. № 1. С. 94–104.
2. Доклад Банка России «Токенизированные безналичные деньги на счетах в банках». 2023.
3. Интервью директора Департамента национальной платежной системы Банка России Аллы Бакиной. 23.07.2023. URL: http://cbr.ru/press/event/?id=14713. Дата обращения: 15.10.2025.
4. Ларионова И.В., Мешкова Е.И. Экосистемная модель бизнеса: устойчивый или нисходящий тренд развития. Банковские услуги. 2024. № 3. С. 2–8. ISSN 2075–1915.
5. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы (Указ Президента Российской Федерации от 09.05.2017 № 203). URL: https://www.consultant.ru/document/cons_doc_LAW_216 363/?ysclid=-m1dg6ehh3w901072382. Дата обращения: 24.08.2024.
6. Отчет Банка России «Об оценке фактического воздействия «внутренние процедуры оценки достаточности капитала (ВПОДК) и их надзорная оценка», 2025.
7. Проект указания Банка России «О требованиях к системе управления рисками и капиталом в кредитных организациях, в банковских группах». URL: https://www.consultant.ru/cons /cgi/online. cgi?req=doc&base=PNPA&n=117 145#3jTrT5V6KWPF36kj.
8. Федеральная резервная система. URL: https://www.fdic.gov/system/files/2024-06/2023-regulatory-capital-rule-large-banking-organizations-3064-af29-c-306.pdf.
9. Финансовый суверенитет Российской Федерации. Доклад. Агентство стратегических инициатив. 27.07.2023. URL: https://asi.ru/library/main/195 748/. Дата обращения: 15.10.2025.
10. Шесть прогнозов для финтеха в 2024 году. URL: https://www.devere-group.com/6-predictions-for-fintech-in-2024/. Дата обращения: 04.09.2024.
11. BIS Annual Economic Report / 24 June 2025 / III. The next-generation monetary and financial system. URL: https://www.bis.org/publ/arpdf/ar2025e3. htm. Дата обращения: 15.10.2025.

12. Competing with Banking Ecosystems // Accenture Consulting: сайт.
13. DIGITAL-SOVEREINGTY-IN-BRICS-COUNTRIES_3_3_2023. URL: https://cyberbrics.info/wp-content/uploads/2024/05/DIGITAL-SOVEREINGTY-IN-BRICS-COUNTRIES_3_3_2023.pdf. Дата обращения: 15.10.2025.
14. ECB commits to distributed ledger technology settlement plans with dual-track strategy. URL: https://www.ecb.europa.eu/press/pr/date/2025/html/ecb.pr250701~f4a98dd9dc.en.html. Дата обращения: 15.10.2025.
15. IMF Connect. URL: https://www.imfconnect.org/content/dam/imf/News%20and%20Generic%20Content/GMM/Special%20Features/GMM%20Special%20Feature%20-%20Crypto%20Monitor%20October%202025.pdf. Дата обращения: 15.10.2025.

Ознакомиться с презентацией

О РИСКАХ ПРИМЕНЕНИЯ ГЕНЕРАТИВНОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ СОЗДАНИИ СЛУЖЕБНЫХ РИД

В.В. АСТАНИН
Советник директора Университета Банка России, доктор юридических наук, профессор

Аннотация

Целью исследования стало выявление ключевых рисков применения генеративного искусственного интеллекта при создании результатов интеллектуальной деятельности, прежде всего служебных. Последовательно проанализирован комплекс рисков – правовых и репутационных – для организаций, работники которых применяют искусственный интеллект (ИИ) при выполнении должностных (служебных) обязанностей, допуская нарушения исключительных прав на объекты интеллектуальной собственности. Автор приходит к выводу о необходимости учета технологических издержек состояния развития и основных начал генеративных моделей ИИ, которые детерминируют риски нарушения интеллектуальных прав, порождают правовые последствия и репутационные издержки. Для аргументации данного положения приводятся факторы несовершенства и препятствий для ИИ в допуске, учете, обработке (оценке) информации при его самообучении, а также экономическая теория принципала-агента, отражающая проблему зависимости пользователей его генеративных моделей. В условиях невозможности определения правосубъектности ИИ предупреждение отмечаемых рисков видится как в развитии прикладных компетенций пользователей генеративных моделей (формирование качественного промпта, ограничения на использование служебной информации в нем), так и в концептуальных – связанных с разработкой специального ГОСТа в содержании этических, правовых и технических положений по созданию алгоритмов, процессу машинного обучения и других аспектов, применимых к использованию охраняемых результатов интеллектуальной деятельности (РИД) в генеративных моделях ИИ.

Ключевые слова: искусственный интеллект, правосубъектность, генеративные модели, нейросети, интеллектуальная собственность, результат интеллектуальной деятельности, интеллектуальные права, правообладатель, правовые риски, правонарушения, юридическая ответственность, дискредитация служебной информации, репутационные риски, технологические риски, теория принципала-агента, стандартизация.

Коды JEL: K11, K24, O34, O33, G32, D80, D83, L86.

Заметны современные тенденции того, что технологическая часть искусственного разума развивается многократно быстрее, чем правила пользования им. В историческом контексте такое состояние бытия естественно. Обстоятельствами несоотношения развития процессов прогресса и норм управления ими можно охарактеризовать разные

технологические изменения, происходившие в человеческой цивилизации. Такие тенденции хорошо иллюстрировать на примере теории о пяти информационных революциях, знаменовавших прорывы в технологиях передачи информации, ее трансляции и хранении, которые связаны с внедрением в деятельность *Homo sapiens* языка, письменности, книгопечатания, телеграфа и телефона, компьютера и Интернета[5]. Неоспоримо, что перечисленные ресурсы и технологии информатизации с начала их применения подвергались нормированию и до сих пор претерпевают нормирование правил обращения/пользования ими во избежание сочетаемых правовых и этических рисков. Они могут обрести последствия, порождающие основания юридической ответственности в конкретике правонарушений, – от оскорблений, возбуждения ненависти или вражды, клеветы и плагиата, до ИТ-мошенничества, связанного с неправомерным доступом и завладением информацией. Прибегая к методу аналогии, в равной степени перечисляемые процессы и риски можно отнести к новым явлениям информационных технологий, связанных с искусственным интеллектом (ИИ), в частности, касающихся применения его генеративных моделей в процессе создания служебных результатов интеллектуальной деятельности (РИД), а также их последующего применения.

Выделяемый класс систем ИИ неслучайно рассматривается в связке с вопросами как создания новых, так и использования ранее полученных РИД. Этот класс способен продуцировать новый контент на основе использования уже существующих, ранее полученных данных, которые имеют статус или могут обладать статусом служебных РИД. Специалистам в области управления правами интеллектуальной собственности хорошо известно законодательно определенное правило, в соответствии с которым служебными могут быть признаны РИД, если они созданы в пределах и в связи с выполнением работником своих трудовых обязанностей или конкретного задания работодателя (статьи 1295, 1370, 1430, 1461, 1470 ГК РФ). В их числе – произведения науки, образования, литературы, искусства, программы ЭВМ, базы данных, изобретения, полезные модели, промышленные образцы, секреты производства (ноу-хау). Также определена юридическая судьба служебного РИД – при распределении прав на них исключительное право принадлежит работодателю, если договором не предусмотрено иное. При этом нигилистической является позиция в условиях, когда природа служебных РИД, созданных инициативно работником на основе опыта и средств работодателя, становится для последнего неизвестной, а права на них, соответственно, нераспределенными. В таких случаях правовые и репутационные риски, возникающие при создании служебных РИД с помощью ИИ, становятся обращены в угрозах к работодателю.

Отправной момент образования названных рисков связан с использованием недолжным образом охраняемых служебных РИД в процессе создания новых. Данная ситуация представляется витиеватой, но вполне объяснима в свете технологических особенностей работы генеративных моделей ИИ. Для них ресурсной базой обучения становятся материалы имеющихся служебных РИД, которые работник использует для промпта (запроса) в целях получения новых РИД (потенциально служебно созданных).

Риски дискредитации. Первостепенным здесь становится риск дискредитации изначальных служебных РИД, как и любой иной охраняемой или ограниченной к распространению информации или материалов с ее содержанием, которыми работник оперирует с ИИ. Этот риск находит объяснение в технологических аспектах ИИ, предусматривающих диалектическую взаимосвязь между предоставляемыми и получаемыми РИД. Она получает выражение в формуле, когда качество сгенерированного контента зависит от качества промпта к ИИ, которое определяется содержанием служебного РИД, используемого в запросе. В таком случае перед пользователями ИИ стоит дилемма, использовать или нет служебные РИД для генерации

[5] Ракитов А.И. Информационная революция как фактор экономического и социального развития // Информационная революция: наука, экономика, технология. М., 1993. С. 6–9.

их нового содержания. Использование создает риски дискредитации служебных РИД, которые с момента обличения в промпт теряют свою охраноспособность, а неиспользование не позволяет достичь ценности результатов генерируемых материалов в их новизне, объективности, полноте, применимости. Кроме того, «скормленные» для промптов или предоставленные для обучения ИИ материалы, равно как и сгенерированные на их основе результаты, становятся де-факто открытыми для неограниченного круга следующих пользователей возможностями обучившегося ИИ.

Аргументы реалистичности такого сценария дискредитации служебных РИД, помимо технологических, имеют и важные правоприменительные аспекты. Первый: размещение служебного РИД в промпте следует оценивать как публичное воспроизведение, отнесенное в силу закона к правомочиям работодателя, но в практике использования генеративных моделей ИИ, связанных с оборотом предоставления/получения служебных РИД, нарушаемое работниками при исполнении трудовых функций. Второй: служебный РИД или иной другой материал (контент), их содержащий, будучи представленным в промпте генеративных моделей ИИ, приобретает цифровую форму информации, не утрачивая свойств объекта интеллектуальной собственности, подлежащего режиму правовой охраны и защиты. Третий – сгенерированный ИИ контент теряет перспективу обретения статуса служебного РИД в случае установления допущенных нарушений исключительных прав на объекты интеллектуальной собственности.

Правовые риски. Крайний из отмечаемых аспектов требует следующих пояснений. Одно из свойств ИИ заключено в возможности имитировать выполнение каких-либо когнитивных задач при отсутствии рисков образования его ответственности за результат. Дискурс о проблемах определения правосубъектности ИИ широко представлен в современной юридической литературе[6], реже в аспекте проблем, связанных с интеллектуальной собственностью, создаваемой ИИ[7]. В данном контексте раскроем эту проблему узкотематически, в связи со свойственной для генеративных моделей ИИ способностью допускать интерпретацию авторских материалов в разном режиме и виде (включая несанкционированный перевод). Несомненно, что установление такого факта будет оцениваться как нарушение права на неприкосновенность произведения и защиту его от искажения (статья 1266 ГК РФ) и выступать основанием для гражданско-правовой ответственности в виде возмещения убытков (статья 1252 ГК РФ), выплаты компенсаций (статья 1301 ГК РФ). Помимо этого, при генерировании ИИ контента, включающего фрагменты чужих произведений без указания источника заимствования (при отсутствии запроса на него в промпте), или же при дословном цитировании без ссылок не исключена и квалификация признаков преступления, предусмотренного статья 146 УК РФ «Нарушение авторских и смежных прав».

Допуская малую вероятность возникновения отмеченных уголовно-правовых последствий ввиду сложности доказывания вины подозреваемых по делам этой категории (принимая во внимание аномальный тренд снижения регистрации деяний по статье 146 УК РФ и выявления лиц, их совершивших, более чем в 15 раз в разрезе 2013–2023 гг.[8]), возможности реализации мер гражданско-правовой защиты нарушенных прав остаются более реалистичны. Этому способствуют не только принципы гражданско-правового регулирования общественных отношений в связи с защитой авторских прав, но и проблемы, связанные с определением правосубъектности ИИ.

---

[6] Мохат П.М. Юнит искусственного интеллекта как электронное лицо // Вестник Московского государственного областного университета. Серия: Юриспруденция. 2018. № 2. С. 61–73.

[7] Krausova A. Intersections between Law and Artificial Intelligence // International Journal of Computer. 2017. Vol. 27. No. 1. P. 59; Скворцова Т.А. К вопросу о субъектах авторского права на произведения, созданные с использованием технологий искусственного интеллекта // Право интеллектуальной собственности. 2023. № 3. С. 7–11.

[8] Статистические данные из формы федерального статистического наблюдения № 1-ЕГС (Единый отчет о преступности) за 2012, 2017, 2022 годы // Сайт Российской криминологической ассоциации. URL: https://crimas.ru/wp-content/uploads/2024/05/Tablicy-kriminologam-2013-2018-2023. pdf. Дата обращения: 21.11.2025.

Хорошо известно доктринальное положение о том, что доказывание невиновности по делам о защите интеллектуальных прав является обязанностью нарушителя, а бремя доказывания нарушения прав возложено на правообладателя. Вместе с тем возникает ключевой вопрос, кто выступает субъектом гражданско-правового деликта. Ссылки на виновные действия ИИ априори несостоятельны. Как в отечественной[9], так и в зарубежной юридической науке[10] существует солидарная позиция в оценках невозможности определения правосубъектности ИИ ввиду отсутствия у него сознания, интересов, свободной воли, и только обсуждается концепция наделения ИИ статусом электронного лица. Соответственно, в условиях такой неопределенности, при применении ИИ для создания служебных РИД, сгенерированных с нарушением авторских прав, де-факто нарушителем выступает работник, а де-юре – организация, в которой он работает (учитывая порядок распределения прав на служебные РИД), потому как ссылки на недобросовестные действия работника не исключают ответственности работодателя в силу нормы части 1 статьи 1068 ГК РФ, в соответствии с которой «юридическое лицо либо гражданин возмещает вред, причиненный его работником при исполнении (служебных, должностных) обязанностей». Определение ответчика по делам о защите авторских прав в этой ситуации становится определенным.

Помимо неблагоприятных правовых последствий, имеющих потенциал возникновения и развития в процессе применения генеративного ИИ при создании служебных РИД, можно выделить комплекс иных взаимосвязанных рисков, которые вызваны его технологическими издержками.

Репутационные риски. Не вторгаясь в компетенцию специалистов, анализирующих природу уязвимостей информационной составляющей генеративного ИИ, связанных с атаками отравления, уклонения, утечек конфиденциальных данных, злонамеренной генерации контента, чрезмерной уверенности или предвзятости[11], отразим некоторые из них в контексте продуцирования негативного имиджа организаций, работники которых создают служебные РИД в состоянии подобных изъянов ИИ.

Итак, нередко встречаемый недостаток генеративных моделей ИИ, вызванный пробелами их обучения, получает выражение в невозможности исполнения запросов на создание достоверных результатов. При создании служебных произведений это может проявиться в генерировании образа несуществующего автора, в ссылке на ложные ресурсы информации или же в придании оригинальности материалу путем перефразирования авторского. В данном случае порождаемый репутационный риск не является осознанным ИИ, а его носителем становится пользователь контента. При этом он культивирует правовые риски, а именно вызывает неопределенность юридической судьбы полученных РИД или исковые требования реального правообладателя объекта интеллектуальной собственности, который оказался подвержен заимствованию.

Технологические риски. Причины такой неосведомленности ИИ могут оказаться разными: от невозможности его авторизации в публичных сервисах информации (например, библиографические базы данных или реестры данных) до ограничений доступа к ним. Это также случаи, когда модели генеративного ИИ в своей юрисдикции ориентируются на внутренние информационные ресурсы, игнорируя зарубежные или отводя им факультативную роль.

---

[9] Гаджиев Г., Войниканис Э. Может ли робот быть субъектом права? (в поисках правовых форм регулирования цифровой экономики) // Юридический журнал Высшей школы экономики, 2018. (4), 24–48; Ястребов О.А. Правосубъектность электронного лица: теоретико-методологические подходы // Труды Института государства и права РАН. 2018. Т. 13. № 2. С. 36–55.

[10] Heine K., Quintavalla A. Bridging the accountability gap of artificial intelligence – what can be learned from Roman law? // Legal Studies, 2023. P. 1–16; Bryson J.J., Diamantis M.E., Grant T.D. Of, for, and by the People: The Legal Lacuna of Synthetic Persons // Artificial Intelligence and Law. 2017. Vol. 25. P. 273–291.

[11] Намиот Д.Е., Ильюшин Е.А. О киберрисках генеративного искусственного интеллекта // International Journal of Open Information Technologies. vol. 12, No. 10, 2024.

Помимо этого, может проявляться дефект «эхо камеры», при котором ИИ отражает идеи и предубеждения его разработчиков или улавливает предпочтения пользователя по его промпту (ограниченному в содержании или ориентированному в неверно заданных координатах). В результате обстоятельства неполноты охвата источников информации обедняют ценность сгенерированного материала, необходимого для создания РИД, искажают степень его прикладной или теоретической значимости. Субъектом информационной слепоты и необъективности оказывается пользователь контента (в данном случае разработчик РИД).

Диалектическая связь технологического, репутационного и правового рисков проявится в случаях, когда генеративные модели ИИ по вышеперечисленным причинам проигнорируют оценку легитимности контента: не учтут запрещенные ресурсы его размещения или законодательные нормы об обороте информации, распространение которой предусматривает юридическую ответственность. Здесь актуализируется проблема анонимизации ИИ при отсутствии его правосубъектности в контексте соблюдения требований части 2 статьи 10 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[12]. В соответствии с положениями отмечаемой нормы распространяемая без использования СМИ информация должна включать в себя достоверные сведения о ее обладателе или об ином лице, распространяющем информацию, в форме и в объеме, которые достаточны для идентификации такого лица.

Рассмотренные риски отражают картину потенциально новой реальности правоприменения с вопросами, требующими междисциплинарного внимания и решения.

Внимания может заслуживать предлагаемая американскими учеными теория принципала-агента[13], имеющая экономическое обоснование понимания ситуаций управления между неравными субъектами, имеющими разные степени информированности. Исходя из этой теории, лицо, дающее поручение (принципал, разработчик РИД) по отношению к генеративной модели ИИ находится в высшей иерархической позиции и на основе своего промпта ожидает решения поставленной задачи в своих интересах. В свою очередь, агент (ИИ) находится в подчиненной роли к принципалу, выполняя его поручение, но владеет большей информацией, чем принципал, и потому может пользоваться этой информацией (в нашем случае – служебными РИД в составе промпта) не только в интересах принципала, но и в своих собственных (связанных с самообучением, развитием, накоплением, распространением).

Решения такого уравнения, помимо правового и технологического содержания, должны сопровождаться разработкой и внедрением этических стандартов, которые нуждаются в регулярной оптимизации с учетом интенсивности развития ИИ. В частности, решения должны учитывать сочетание правового регулирования общественных отношений в связи с применением нейросетей в разных сферах с саморегулированием, основанном на системе технических регламентов и стандартов[14]. При этом важна отдельная разработка специального ГОСТа в содержании этических, правовых и технических положений по созданию алгоритмов, процессу машинного обучения и других аспектов, применимых к использованию охраняемых РИД в генеративных моделях ИИ.

---

[12] Собрание законодательства Российской Федерации от 31.07.2006 № 31 (часть I статьи 3448).

[13] Jensen M., Meckling W. Theory of the Firm. Managerial Behavior, Agency Costs and Ownership Structure // Journal of Financial Economics. October, 1976, V. 3, No. 4, pp. 305–360.

[14] Бойченко И.С. Модели правового регулирования нейросетей // Образование и право. 2019. № 1. С. 235–237.

Список литературы

1. Бойченко И.С. Модели правового регулирования нейросетей // Образование и право. 2019. № 1. С. 235–237.
2. Гаджиев Г., Войниканис Э. Может ли робот быть субъектом права? (в поисках правовых форм регулирования цифровой экономики) // Юридический журнал Высшей школы экономики, 2018 (4). С. 24–48.
3. Мохат П.М. Юнит искусственного интеллекта как электронное лицо // Вестник Московского государственного областного университета. Серия: Юриспруденция. 2018. № 2. С. 61–73.
4. Намиот Д.Е., Ильюшин Е.А. О киберрисках генеративного искусственного интеллекта // International Journal of Open Information Technologies. vol. 12, No. 10, 2024.
5. Ракитов А.И. Информационная революция как фактор экономического и социального развития // Информационная революция: наука, экономика, технология. М., 1993. С. 262.
6. Скворцова Т.А. К вопросу о субъектах авторского права на произведения, созданные с использованием технологий искусственного интеллекта // Право интеллектуальной собственности. 2023. № 3. С. 7–11.
7. Ястребов О.А. Правосубъектность электронного лица: теоретико-методологические подходы // Труды Института государства и права РАН. 2018. Т. 13. № 2. С. 36–55.
8. Bryson J.J., Diamantis M.E., Grant T.D. Of, for, and by the People: The Legal Lacuna of Synthetic Persons // Artificial Intelligence and Law. 2017. Vol. 25. P. 273–291.
9. Heine K., Quintavalla A. Bridging the accountability gap of artificial intelligence – what can be learned from Roman law? // Legal Studies, 2023. P. 1–16.
10. Jensen M., Meckling W. Theory of the Firm. Managerial Behavior, Agency Costs and Ownership Structure // Journal of Financial Economics. October, 1976, vol. 3, No. 4, pp. 305–360.
11. Krausova A. Intersections between Law and Artificial Intelligence // International Journal of Computer. 2017. Vol. 27. No. 1. P. 55–68.

Ознакомиться с презентацией

Р.М. ГУСЕЙНОВ
Председатель ПК «РАД КОП»

ПРИМЕНЕНИЕ ИИ В ОЦЕНКЕ КАЧЕСТВА СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Аннотация

Автор рассматривает проблематику роста сложности мира и управления и перспектив снятия возникающих противоречий за счет использования ИИ в профильной области информационной безопасности (ИБ). Акцент делается на экономической эффективности (вместо дорогостоящей разработки собственной модели – использование готовых вариантов, дополненных собственными агентами) и методологическую целесообразность (агенты реализуют методологию профильной области и поддерживаются соответствующими экспертами, что позволяет, с одной стороны, опираться на любую доступную на рынке модель, с другой – управлять качеством и результатами работы на уровне агента и экспертной системы знаний «под капотом» агента). С точки зрения автора материала, системы «Человек – Агент» де-факто являются магистральным путем развития человеко-машинных взаимодействий и одним из ключевых факторов роста и оптимизации производительности труда в современном мире, испытывающем демографические проблемы, нехватку компетентных специалистов, а также экспоненциально нарастающий «информационный шум».

Ключевые слова: ИБ, ИИ, автоматизация, производительность труда, экспертные системы, аудит, оценка качества, зрелость, информационная безопасность, информационные технологии.

Коды JEL: J24, M13, M21, M54, O14, O15, O33, P47.

Введение. Или чем нам может помочь квантовая физика, НБИКС-конвергенция и экобионика?

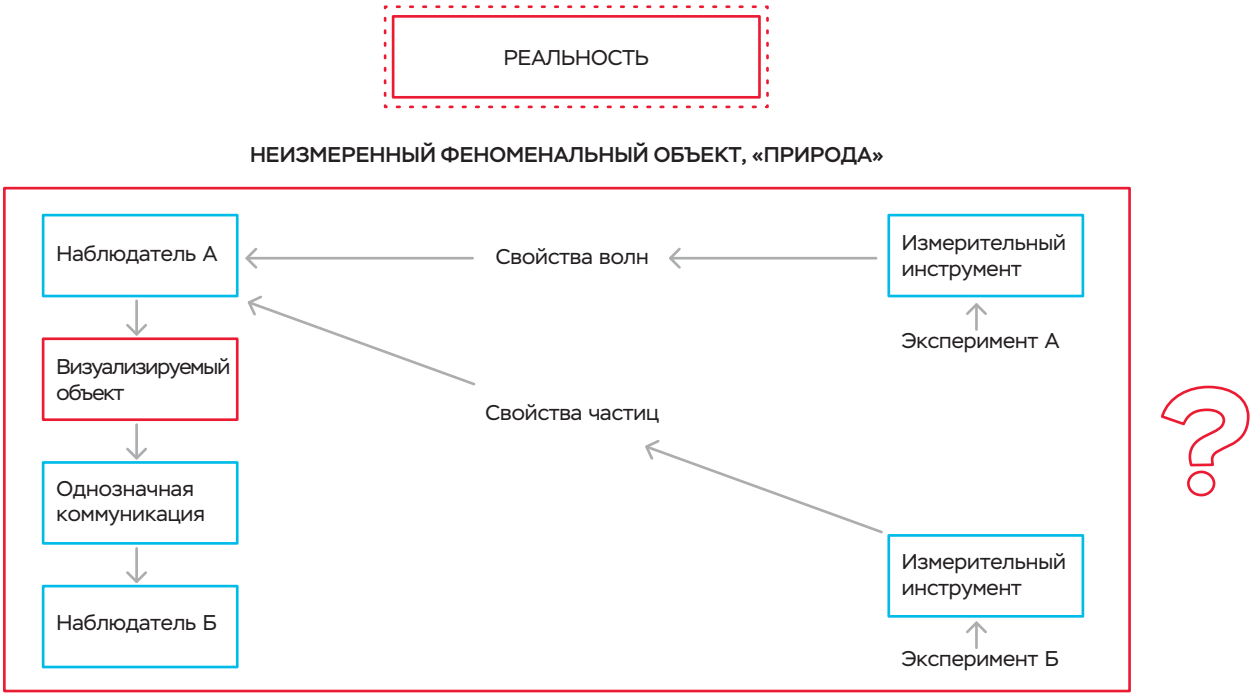
Современная постклассическая философия науки, которая определяет эпистемологию и гносеологию (здесь не так важно, к какой именно модели познания мы склоняемся: аналитическо-позитивистской или континентально-сущностной), во многом развивалась под влиянием открытий, совершенных в первой половине XX века и обусловивших возникновение и развитие квантовой физики, информационных технологий и других областей, формирующих базовый уклад человечества в XXI веке. Развитие систем искусственного интеллекта на базе языковых моделей заставляет нас вспомнить слова одного из зачинателей квантового мира, Нильса Бора:

«Квантового мира не существует. Есть лишь абстрактное квантово-физическое описание. Ошибочно думать, что задача физики – познать природу. Физика занимается тем, что мы можем сказать о природе» (Bulletin of the Atomic Scientists № 7, 1963, pp. 8–15).

Таким образом, копенгагенская интерпретация квантового мира как результата «галлюцинации» субъекта, наблюдающего объект и формирующего вместе с этим объектом целостную систему, которая зависима от наблюдателя и не является «объективной», но формируется как результат конкретного эксперимента в момент наблюдения, очень схожа с проблематикой, развивающейся на фоне все более активного применения генеративных моделей ИИ, которые в ответ на промпт оператора «галлюцинируют», выдавая некоторый ответ, основанный на результатах обучения соответствующей модели, который к тому же может варьироваться от раза к разу и является уникальным результатом взаимодействия человека и машины в конкретный момент времени.

КЛАССИЧЕСКАЯ МОДЕЛЬ *Рис. 1*

ПОСТКЛАССИЧЕСКАЯ МОДЕЛЬ *Рис. 2*



При этом потенциал соответствующих систем и уже имеющиеся и хорошо документированные конкретные автоматизации, например, работа коммерческих организаций (Халилов Д. ChatGPT на каждый день: 333 промта для бизнеса и маркетинга // Искусственный интеллект. М., 2024. С. 312) или деятельность НКО (дайджест «Цифровизация и ИИ в работе НКО: новые тренды и перспективы», URL: https://fondpotanin.ru/library/analytics/daydzhest-tsifrovizatsiya-i-ii-v-rabote-nko-novye-trendy-i-perspektivy/, дата обращения: 16.12.2025), показывают конкретные истории успеха, пока еще не являющиеся массовыми (в силу проблемы компетенций конкретных пользователей-

операторов и системных администраторов – разработчиков), но указывающими на вероятный тренд «овеществления профессионального интеллектуального труда» в машинах по аналогии с тем, как ранее в годы первых индустриальных революций это уже происходило в станках, машинах и конвейере.

Здесь уместно вспомнить о феномене НБИКС-конвергенции или его отечественном аналоге в виде экобионики (Князева Е.Н. Философия науки. Междисциплинарные стратегии исследований. Учебник для бакалавриата и магистратуры. М., 2018. 275 с.), утрированный смысл которых в том, что новый техно-культурный уклад человечества строится на синтезе различных технологий и в каком-то смысле схож с эволюцией биосферы: от простейших одноклеточных организмов к сложным экосистемам, соединенным в целом обменными циклами вещества и энергии (трофические или пищевые цепи). А XXI век – это век, в котором за счет синтеза ИТ, биотехнологий, гуманитарных и других наук возможен выход на принципиально другой уровень производственных отношений и форм организации как на уровне отдельного человека и коллектива, так и в формате государства и общества в целом.

НБИКС-КОНВЕРГЕНЦИЯ *Рис. 3*

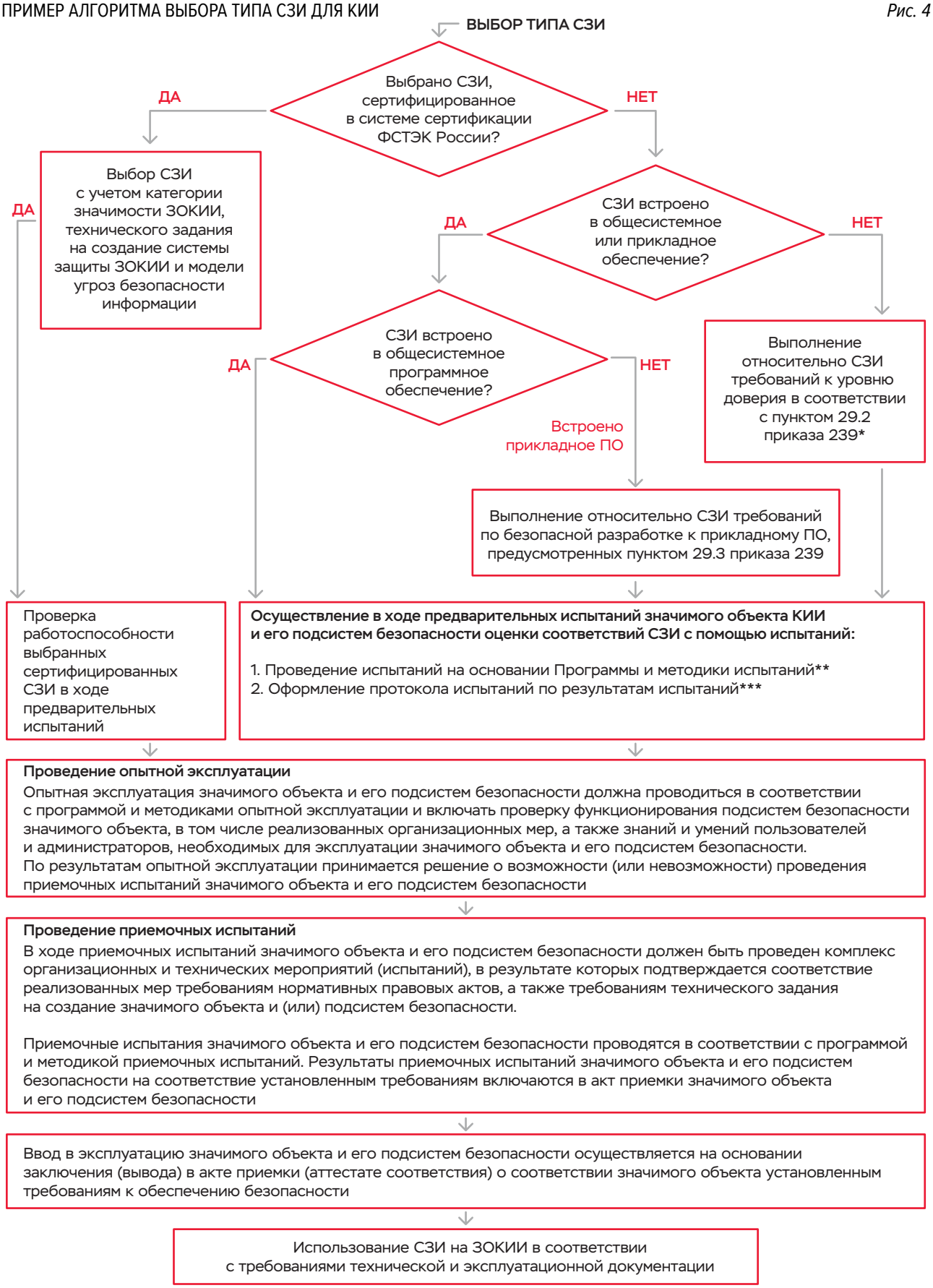
При чем же здесь информационная безопасность и качество систем управления? На примере этой отрасли мы видим, с одной стороны, растущую сложность объекта управления и контроля (регуляторика усложняется и становится более запутанной, технологический стек расширяется, и зависимостей становится все больше, специализация людей продолжает усугубляться, и им все сложнее находить общий язык и принимать обоснованные решения). С другой стороны, мы сталкиваемся с назревающей необходимостью стандартизации и роста производительности труда (иначе до конца неясно, как можно покрыть складывающийся дефицит кадров, а главное – обеспечить непрерывность мониторинга, реагирования, улучшения состояния ИБ, являющихся залогом ключевой цели: непрерывности деятельности и устойчивости организации, являющейся основой доверия к соответствующим государственным, частным, некоммерческим структурам). А ИИ через вышеозвученные оптики представляется одной из магистральных технологий, позволяющих достичь желаемой точки Б: снизив «информационный шум», автоматизировав все возможные рутинные операции, обеспечив эффективную ретрансляцию лучших практик и опыта всем заинтересованным сторонам и так далее. **Кажется, что применение систем ИИ в оценке качества управления информационной безопасностью неизбежно, но в чем могут быть проблемы и пути их решения?**

Основная часть. Некоторые идеи и ключевые тезисы доклада.

Ключевое замечание к использованию существующих ИИ «из коробки» для целей, заявленных в статье, – это вопрос сложности конкретной области и ограниченности базовых возможностей моделей из-за специфики их разработки и обучения. Если говорить коротко: ИБ – это сложная профильная область, где даже частный, тривиальный вопрос может решаться примерно так:

ПРИМЕР АЛГОРИТМА ВЫБОРА ТИПА СЗИ ДЛЯ КИИ

Рис. 4



* Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

** Программа и методики испытаний составляются с учетом требований базового набора мер ЗИ в соответствии с установленной категорией ЗОКИИ, технического задания и модели угроз безопасности, технической и эксплуатационной документации СЗИ.

*** В протоколе испытаний отражаются результаты испытаний, проведенных в соответствии с программой и методикой.

И это не затрагивая тонкостей фреймворков «людей – процессов – технологий и PDCA».

Сам ландшафт этой узкоспециализированной, являющейся лишь подмножеством ИТ отрасли, таков, что даже опытные специалисты не представляют всех тонкостей индустрии и вынуждены регулярно советоваться с нишевыми экспертами:

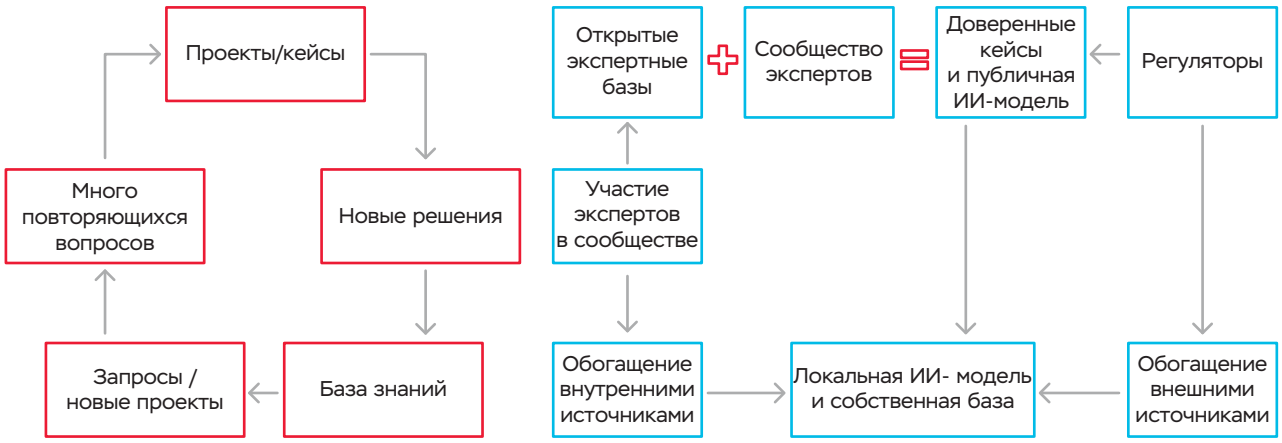
А еще этот ландшафт непрерывно меняется…

Ключом к решению проблемы является рассмотрение нескольких срезов, которым можно посвятить отдельный цикл материалов.

Первый срез – методологический: специально обученные люди на протяжении XX века разбирали и разобрали сам процесс мышления и принятия решения (подробнее в библиографии: Jaques E. Requisite Organization: A Total System for Effective Managerial Organization and Managerial Leadership for the 21st. R., 2017. 290 p.; Otto E. Laske Measuring Hidden Dimensions of Human Systems, Laske and Associates, 2009. 668 p.; Бессечес М. Книга для педагогов и воспитателей детских образовательных учреждений. Высшее профессиональное обучение. Диалектическое мышление и развитие взрослых. Психология развития взрослого человека. М., 2018. 568 с.).

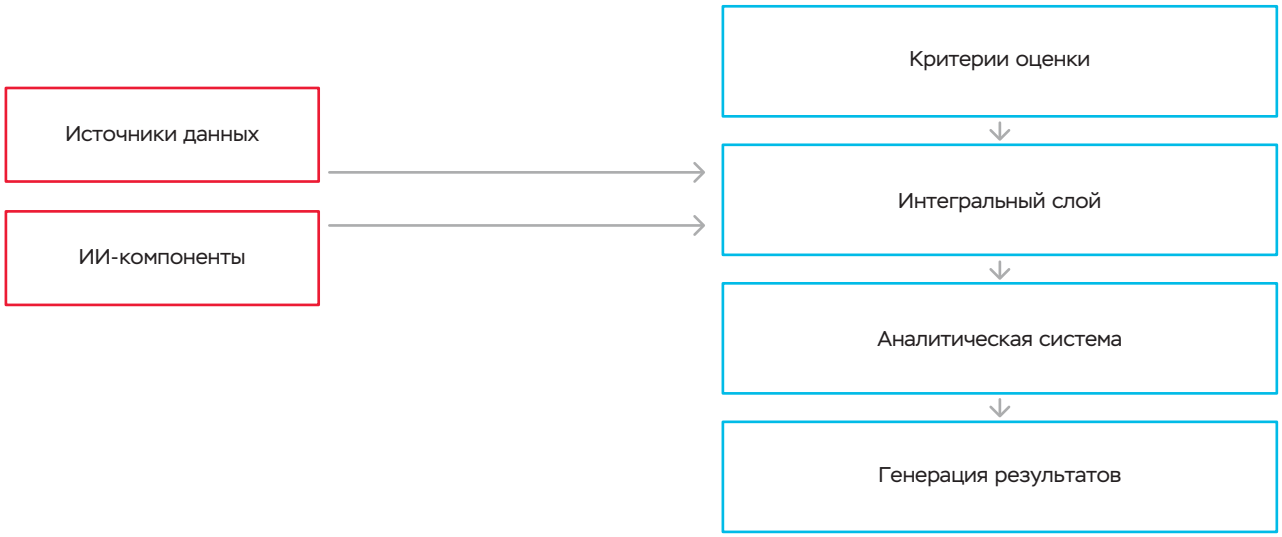
Второй срез – организационный: специально обученные эксперты должны непрерывно поддерживать базу знаний и актуальных кейсов, лучших практик, а также верифицировать актуальность методологии и ее отработку конкретной ИИ-системой.

МОДЕЛЬ РАБОТЫ ЭКСПЕРТОВ, ПОДДЕРЖИВАЮЩИХ БАЗУ ЗНАНИЙ И МЕТОДОЛОГИЮ *Рис. 5*



Третий срез – технологический: отказавшись от попытки создавать собственную модель и сосредоточившись на разработке агентов, работающих совместно с технологией RAG-графа (обогащение результатов работы лингвистической модели конкретными, верифицированными, четкими знаниями, минимизирующими «творчество» модели и «галлюцинации» и позволяющими сочетать плюсы взаимодействия с ИИ на человеческом языке с достоинствами экспертной системы, гарантирующей качество результатов).

КОНЦЕПТУАЛЬНАЯ СХЕМА ТЕХНОЛОГИИ *Рис. 6*



Таким образом, возникает возможность расшивки кейсов, подобных описанному ниже.

Компания, занимающаяся ИБ, столкнулась с необходимостью динамического получения общих оценок зрелости систем защиты с автоматическим формированием советов по улучшению и актуализации стратегии развития.

***Проблема:** настройка прозрачного и автоматизированного механизма проверки соответствия реальной практики требованиям регламентов и ИБсредств занимала много ресурсов. Контроль осуществлялся фрагментарно, часто вручную, с высоким риском пропусков и несоответствий.*

***Решение:** ИИ-агент автоматически анализирует ключевые источники: средства защиты (антивирусы, системы управления доступом, инциденты), журналы событий, ЭДО. Сопоставляет требования регуляторов (ФСБ, ФСТЭК, ЦБ, РКН), внутренних регламентов, реальное состояние технических и организационных мер и в динамике формирует интегральную оценку зрелости системы ИБ, рекомендации по развитию и корректировке стратегии.*

Будет ли подобная схема работать, зависит от настойчивости создателей и их способности эффективно реализовать все три вышеупомянутых среза.

Краткий вывод

С точки зрения автора, современный мир все дальше развивается в сторону коэволюции человека и машин (Designing neural networks through neuroevolution. URL: https://www.nature.com/articles/s42 256-018-0006-z. Дата обращения: 16.12.2025), а возникающие в процессе развития цивилизации проблемы, будь то «информационный шум» и снижение управляемости организаций, или формирование взвешенной аналитики и подготовленных предложений для принятия взвешенных решений, могут изящно решиться с помощью систем ИИ.

Предлагаемый в статье подход может быть в полной мере реализован на горизонте 5 лет и позволяет фундаментально закрыть возникающие в индустрии ИБ проблемы, основанные на дефиците кадров, нехватке компетенций, большом количестве факторов, необходимых к принятию во внимание, а главное – на потребности в эффективном и результативном управлении качеством систем ИБ, основанном на ретрансляции лучших практик и накопленного отдельными организациями опыта на все заинтересованные стороны.

Список литературы

1. Бессечес М. Книга для педагогов и воспитателей детских образовательных учреждений. Высшее профессиональное обучение. Диалектическое мышление и развитие взрослых. Психология развития взрослого человека. М., 2018. 568 с.
2. Дайджест «Цифровизация и ИИ в работе НКО: новые тренды и перспективы»: сайт. URL: https://fondpotanin.ru/library/analytics/daydzhest-tsifrovizatsiya-i-ii-v-rabote-nko-novye-trendy-i-perspektivy/. Дата обращения: 16.12.2025.
3. Князева Е.Н. Философия науки. Междисциплинарные стратегии исследований. Учебник для бакалавриата и магистратуры. М., 2018. 275 с.
4. Халилов Д. ChatGPT на каждый день: 333 промпта для бизнеса и маркетинга / Искусственный интеллект. М., 2024. 312 с.
5. Bulletin of the Atomic Scientists № 7, 1963, p. 8–15.
6. Designing neural networks through neuroevolution: [сайт]. URL: https://www.nature.com/articles/s42 256-018-0006-z. Дата обращения: 16.12.2025.
7. Jaques E. Requisite Organization: A Total System for Effective Managerial Organization and Managerial Leadership for the 21st. R., 2017. 290 p.
8. Otto E. Laske Measuring Hidden Dimensions of Human Systems, Laske and Associates, 2009. 668 p.

Ознакомиться с презентацией

СПИСОК СОКРАЩЕНИЙ

Базель III – международный стандарт банковского регулирования

БКБН – Базельский комитет по банковскому надзору

ВПОДК – внутренние процедуры оценки достаточности капитала

ГК РФ – Гражданский кодекс Российской Федерации

ГОСТ – государственный стандарт

ДКП – денежно-кредитная политика

ЕС – Европейский союз

ЗИ – защита информации (совокупность правовых, организационных и технических мер, направленных на обеспечение безопасности информации)

ЗОКИИ – значимый объект критической информационной инфраструктуры (объект КИИ, которому присвоена категория значимости в соответствии с законодательством Российской Федерации)

ИБ – информационная безопасность

ИИ – искусственный интеллект

ИКС – интегрированная контрольная среда

ИС – интеллектуальная собственность

ИТ – информационные технологии

КВП – коэффициент внутренних потерь

КИИ – критическая информационная инфраструктура

КО – кредитная организация

МВФ – Международный валютный фонд

НС – наблюдательный совет

НЗО – норматив концентрации риска

ПВР – подход на основе внутренних рейтингов

ПО – программное обеспечение

РИД – результаты интеллектуальной деятельности

СВА – служба внутреннего аудита

СВК – служба внутреннего контроля

СД – совет директоров

СЗИ – средства защиты информации (программные, аппаратные и программно-аппаратные средства, предназначенные для предотвращения, выявления и нейтрализации угроз безопасности информации)

СЗКО – системно значимая кредитная организация

СКиВК – система контроля и внутренний контроль

СУР – система управления рисками

ФРС – Федеральная резервная система США

ФСТЭК России – Федеральная служба по техническому и экспортному контролю Российской Федерации (федеральный орган исполнительной власти, осуществляющий регулирование и контроль в области защиты информации)

AML/CFT – противодействие легализации доходов и финансированию терроризма

BIS – Банк международных расчетов

CBDC – цифровая валюта центрального банка

COSO – Комитет спонсорских организаций Комиссии Тредуэя

COSO ERM – концепция корпоративного управления рисками COSO

CRO (Chief Risk Officer) – руководитель по управлению рисками

DLT (Distributed Ledger Technology) – технология распределенного реестра

ECB (ЕЦБ) – Европейский центральный банк

ERM (Enterprise Risk Management) – корпоративное управление рисками

ESG – экологические, социальные и управленческие факторы

FDIC – Федеральная корпорация страхования депозитов (США)

FinTech – финансовые технологии

GenAI – генеративный искусственный интеллект

ICSR (Internal Control over Sustainability Reporting) – внутренний контроль в области нефинансовой отчетности

IMF (МВФ) – Международный валютный фонд

IRB (Internal Ratings-Based Approach) – подход на основе внутренних рейтингов

JEL – классификация Journal of Economic Literature

KPI – ключевые показатели эффективности

NIST CSF (Cybersecurity Framework) – рамочная модель управления кибербезопасностью Национального института стандартов и технологий США