ИИ в компании: чек-лист руководителя по управлению рисками персональной ответственности

Практический инструмент для руководителей

Юлия Ахонина

Май 2026

ВВЕДЕНИЕ

ИИ в компании: чек-лист руководителя по управлению рисками персональной ответственности

Внедрение искусственного интеллекта (ИИ) в бизнес-процессы перестало быть экспериментом. По мере роста масштаба применения увеличивается уровень связанных рисков — финансовых, регуляторных, репутационных. Эти риски выходят за пределы ИТ-функции и становятся частью системы управления и внутреннего контроля.

⚠ Оценка действий руководителя при инцидентах строится на критериях разумности и добросовестности: действовал ли он как обычный разумный руководитель в сопоставимых условиях для обеспечения безопасного и корректного внедрения и использования ИИ в компании.

Цели чек-листа

- Оценить текущий уровень управления внедрением и применением ИИ в компании и выявить зоны риска
- Сформировать минимальный набор необходимых управленческих действий для обеспечения безопасного внедрения и использования ИИ в компании
- Проверить разумность и добросовестность подхода руководителя к внедрению и использованию ИИ в компании

Чек-лист учитывает лучшие на момент его составления практики, носит обобщенный характер и должен применяться с учетом специфики деятельности организации, масштаба и характера используемых ИИ-решений, а также критичности бизнес-процессов, в которых они задействованы.

СТРАТЕГИЯ

1. Утверждена ли стратегия использования ИИ?

Стратегия задает рамку всех решений и подтверждает, что внедрение ИИ носит системный характер. Она должна фиксировать не только цели, но и ограничения: какие задачи исключены из сферы применения ИИ и каков допустимый уровень риска. Регулярный пересмотр стратегии обязателен — технологии и регуляторная среда меняются стремительно.

Стратегия задает рамку всех решений. Ее наличие подтверждает, что внедрение ИИ носит системный характер и связано с целями бизнеса..

Проверьте, что в компании:

- ○ Определены цели использования ИИ
- ○ Зафиксированы допустимые и недопустимые области применения
- ○ Определен уровень допустимого риска
- ○ Стратегия регулярно пересматривается

УПРАВЛЕНИЕ РИСКАМИ

2. Утверждены ли правила управления рисками ИИ?

Правила управления рисками определяют, как компания обеспечивает безопасное использование ИИ на практике. Меры по снижению рисков должны быть конкретными, с назначенными ответственными, а мониторинг — встроен в операционные процессы. Особого внимания требуют вопросы информационной безопасности: ИИ-системы обрабатывают значительные массивы конфиденциальных данных.

⚠ Правила определяют, как именно компания обеспечивает безопасное использование ИИ на практике.

Чек-лист:

- ○ Есть формализованная модель оценки рисков
- ○ Определены меры по снижению рисков
- ○ Назначены ответственные
- ○ Встроен регулярный мониторинг
- ○ Урегулированы вопросы ИБ и работы с данными

РЕЕСТР ИИ

3. Ведется ли полный и актуальный реестр ИИ?

Реестр — основа контроля. Без него невозможно системно управлять рисками.

Реестр должен охватывать не только официально внедренные системы, но и «теневой ИИ» — инструменты, используемые сотрудниками неформально. Публичные ИИ-сервисы могут обрабатывать конфиденциальные корпоративные данные, выходя за пределы информационной безопасности организации.

Что должен включать реестр:

- Все ИИ-решения, официально внедренные в компании
- Процессы, в которых они используются
- Уровни риска для каждого решения
- ИИ-инструменты, создаваемые сотрудниками
- Выявленный и регулируемый «теневой ИИ», вайбкодинг

Чек-лист:

- ◯ Зафиксированы все ИИ-решения
- ◯ Указаны процессы их использования
- ◯ Определены уровни риска
- ◯ Выявлен и регулируется «теневой ИИ»
- ◯ Учитываются решения, создаваемые сотрудниками

РАСПРЕДЕЛЕНИЕ ОТВЕТСТВЕННОСТИ

4. Назначены ли ответственные за ИИ-решения?

Прозрачное распределение ответственности позволяет эффективно реагировать на инциденты. Критически важен человек с правом остановки системы: если нет понимания, кто уполномочен принять это решение, промедление может многократно увеличить ущерб.

Владелец бизнес-процесса

Отвечает за соответствие ИИ-решения бизнес-целям и последствия его применения

Технический владелец

Отвечает за корректность работы модели и техническое обслуживание

Контрольные функции

Риск, ИБ и юристы вовлечены постоянно, а не только при инцидентах

Право остановки

Уполномочен принять решение об экстренном отключении системы

Чек-лист:

- ○ Назначен владелец бизнес-процесса для каждого ИИ-решения
- ○ Назначен технический владелец
- ○ Контрольные функции (риск, ИБ, юристы) вовлечены на постоянной основе
- ○ Определено лицо с правом остановки системы
- ○ Описана процедура экстренного отключения

ПРЕДВАРИТЕЛЬНАЯ ОЦЕНКА

5. Проводится ли оценка рисков до запуска каждого ИИ-решения?

Предварительная оценка подтверждает, что решение о внедрении было разумным и обоснованным. Если что-то пойдет не так, именно документация предварительной оценки позволит показать, что риски были проанализированы заранее. Объяснимость решений должна оцениваться заблаговременно — если модель принимает решения, которые невозможно объяснить регулятору или клиенту, это само по себе существенный риск.

Оценка влияния

Анализ последствий для клиентов и бизнес-процессов

Анализ данных

Качество, полнота, актуальность, соответствие законодательству о персональных данных

Определение ущерба

Выявление максимально возможных негативных последствий

Оценка объяснимости

Проверка возможности объяснить результаты ИИ клиентам и регуляторам

Стоп-факторы

Условия, при которых запуск ИИ-решения недопустим

Чек-лист:

- ○ Проводится оценка влияния на клиентов и бизнес-процессы
- ○ Анализируются используемые данные (качество, полнота, соответствие законодательству)
- ○ Определен потенциальный максимальный ущерб
- ○ Оценена объяснимость решений ИИ
- ○ Зафиксированы стоп-факторы запуска
- ○ Результаты оценки документируются

ЖИЗНЕННЫЙ ЦИКЛ

6. Охвачен ли контролем весь жизненный цикл ИИ?

Основные риски возникают после запуска — модели деградируют, данные устаревают, условия применения меняются. Контроль должен осуществляться на каждом этапе. Каждое значимое изменение модели должно проходить через тот же цикл оценки, что и первоначальное внедрение.

Разработка и тестирование

Создание и валидация моделей до выхода в продуктив

Внедрение

Развертывание с документированием решений и рисков

Регулярный мониторинг

Проверка производительности и уровня риска

Отслеживание деградации

Выявление отклонений и дрейфа модели

Изменения и вывод

Процедуры обновления и завершения использования

ⓘ Непрерывный мониторинг жизненного цикла ИИ — практический инструмент снижения операционных и правовых рисков.

Чек-лист:

- ○ Контроль осуществляется на всех этапах жизненного цикла
- ○ Каждое изменение модели проходит цикл оценки
- ○ Настроено отслеживание деградации модели
- ○ Определены пороговые значения для эскалации
- ○ Регламентирована процедура вывода ИИ-решения из использования

КОНТРОЛЬ И ПРОЗРАЧНОСТЬ

7–8. Объяснимость решений и роль человека

7. Обеспечена ли объяснимость решений ИИ?

Если компания не может объяснить, почему ИИ принял то или иное решение, это создает серьезную правовую уязвимость. Регуляторы и суды все чаще требуют именно такой прозрачности. Для непрозрачных моделей («чёрный ящик») необходимо предусмотреть специальные компенсирующие меры контроля.

- ○ Сотрудники понимают результаты ИИ
- ○ Проводится регулярный внутренний аудит решений
- ○ Можно объяснить решения клиентам и регуляторам
- ○ Предусмотрены меры для непрозрачных моделей

8. Закреплена ли роль человека в критических решениях?

В высокорисковых процессах — кредитование, оценка персонала, юридически значимые решения — полная автоматизация недопустима. Человек должен реально оценивать решение ИИ, а не формально его подтверждать.

- ○ Определены зоны обязательного участия человека
- ○ Исключена полная автоматизация в высокорисковых процессах
- ○ Настроен контроль автономных решений
- ○ Определен порядок вмешательства

ИНЦИДЕНТЫ

9. Ведется ли учет ИИ-инцидентов?

Журнал инцидентов — одно из наиболее убедительных доказательств добросовестного поведения руководителя: он демонстрирует, что организация не только выявляла проблемы, но и реагировала на них. Каждый инцидент должен проходить полный цикл. Для наиболее серьезных случаев предусмотрена эскалация на уровень топ-менеджмента.

Фиксация

Все инциденты регистрируются в едином журнале без исключений

Анализ

Определяются первопричины, а не только симптомы произошедшего

Меры

Корректирующие действия с ответственными и сроками исполнения

Эскалация

Критические случаи передаются на уровень топ-менеджмента немедленно

Чек-лист:

- ○ Ведется единый журнал ИИ-инцидентов
- ○ Фиксируются все инциденты без исключений
- ○ Проводится анализ первопричин
- ○ Определены корректирующие меры с ответственными и сроками
- ○ Предусмотрена эскалация критических случаев на уровень топ-менеджмента
- ○ Отслеживается эффективность принятых мер

УПРАВЛЕНИЕ ПОСТАВЩИКАМИ

10. Выстроена ли работа с поставщиками ИИ?

Использование внешних решений не снижает ответственность компании перед клиентами и регуляторами. Работа с поставщиками ИИ должна быть выстроена столь же строго, как и управление собственными разработками. Договорное закрепление ключевых условий — реальный инструмент управления рисками, а не формальность.

Пять требований к поставщику:

Идентификация ИИ

Определить, где и как используется ИИ в решениях поставщика

Оценка рисков

По тем же стандартам, что и для внутренних систем

Информация о модели

Достаточный объем сведений для управления рисками

Договорная защита

Ответственность, ИС, данные, безопасность, уведомления

Постдеплойный мониторинг

Непрерывный контроль на протяжении всего срока использования

Ключевые договорные условия:

- Распределение ответственности за ошибки модели
- Права на интеллектуальную собственность
- Запрет использования данных организации для обучения
- Порядок уведомления об изменениях в модели
- Требования к безопасности и возможность проверки
- Условия расторжения и прекращения договора

ПЕРСОНАЛЬНАЯ ОТВЕТСТВЕННОСТЬ

11. Сформирована ли «папка защиты» руководителя?

Риски персональной ответственности могут реализовываться спустя годы после принятия решения. Вспомнить обстоятельства и найти документы, подтверждающие разумность действий, бывает крайне сложно — особенно если руководитель сменил место работы. Личный файл с ключевыми документами — важнейшая практическая рекомендация.

Стратегия и политики

Стратегия ИИ, правила управления рисками, внутренние политики

Реестр и оценки

Реестр ИИ, материалы оценки рисков, стоп-факторы запуска

Протоколы и договоры

Протоколы согласований, документы по выбору поставщика, договоры

Мониторинг и аудит

Результаты мониторинга, журналы инцидентов, материалы внутреннего аудита

Руководитель, системно формирующий «папку защиты», создает надежную доказательную базу разумности и добросовестности — важнейший инструмент защиты от персональной ответственности.

ИТОГ

Минимальный стандарт разумного руководителя

Знать, где используется ИИ

Полный и актуальный реестр всех ИИ-решений, включая теневой ИИ

Понимать риски

Системная оценка рисков на всех этапах жизненного цикла ИИ

Обеспечить контроль

Объяснимость решений, участие человека и непрерывный мониторинг

Фиксировать и действовать

Документировать решения, инциденты и меры по их минимизации

Соответствие данному стандарту — не только обеспечение безопасного внедрения и использования ИИ для компании, но и практическая защита от персональной ответственности в случае претензий со стороны акционеров, клиентов, контрагентов и регулятора.

ОБ АВТОРЕ

Юлия Ахонина

К.ю.н. · Управление рисками для руководителей · LegalTech · Legal Operations

---

Практикующий юрист с 17-летним опытом в международном консалтинге. Преподаватель СПбГУ.

Методолог исследований «Технологии Доверия»: Бенчмаркинг юридических функций 2024–2025, «Созвездие "Конструктор договоров"».

В рейтингах: Право300, Пробанкротство, Коммерсант.

Банкротство

Поддержка бизнеса и менеджмента в кризисных ситуациях

LegalOps и LegalTech

Анализ юридических функций, внедрение ИИ

akhonina-legal.tech

Email: Yulia.akhonina@gmail.com