Технологии
и Решения

Шаблон политики ответственного использования ИИ

8 разделов · Базовый шаблон для адаптации под вашу компанию

Политика ответственного ИИ определяет принципы и правила разработки, внедрения и использования ИИ-систем в компании. Без такой политики каждый сотрудник использует ИИ по-своему — с непредсказуемыми рисками. Этот шаблон можно адаптировать за 1—2 дня.

Для кого

- CTO, CDO, руководители ИИ-проектов
- Юристы и комплаенс-специалисты
- HR-директора (обучение сотрудников)
- Члены комитетов по рискам и технологиям

Что внутри

- 8 разделов: от принципов до санкций
- Классификация ИИ-систем по уровням риска
- Правила использования внешних ИИ (ChatGPT, Claude)
- Процесс внедрения новых ИИ-систем (5 шагов)
- Готовые формулировки — адаптируйте под свою компанию

Как пользоваться

- Прочитайте все 8 разделов, отметьте релевантные для вас
- Адаптируйте формулировки под вашу отрасль и масштаб
- Согласуйте с юристом и CTO, утвердите на уровне CEO/СД

1. Цель и область применения

- Цели: обеспечение безопасного, этичного и законного использования ИИ
- Область: все подразделения, сотрудники, подрядчики
- Связь с политиками: информационная безопасность, ПДн, этика

2. Принципы ответственного ИИ

- Прозрачность: пользователи знают, когда взаимодействуют с ИИ
- Справедливость: ИИ не дискриминирует по полу, возрасту, национальности
- Подотчётность: за каждой системой закреплён ответственный
- Конфиденциальность: данные защищены по законодательству
- Безопасность: ИИ проходит тестирование перед запуском

3. Классификация ИИ-систем по риску

- Низкий риск: внутренние задачи (тексты, аналитика) — уведомительный режим
- Средний: влияние на клиентов (рекомендации, чат-боты) — согласование
- Высокий: решения о людях (HR, кредитный скоринг) — утверждение комитетом

4. Правила использования внешних ИИ-сервисов

- Запрещено: ПДн, коммерческая тайна, финансы — в облачные ИИ без анонимизации
- Разрешено: генерация текстов, формул, анализ публичной информации
- Обязательно: проверка всех результатов ИИ перед использованием
- Рекомендовано: локальные модели для конфиденциальных данных

5. Процесс внедрения новых ИИ-систем

- Шаг 1: Заявка (описание, данные, риски, ожидаемый эффект)
- Шаг 2: Оценка рисков (безопасность, приватность, предвзятость)
- Шаг 3: Пилот (ограниченная группа, 2—4 недели)
- Шаг 4: Утверждение (руководитель + AI governance)
- Шаг 5: Мониторинг (метрики, инциденты, обратная связь)

6. Мониторинг и аудит

- Аудит: не реже 1 раза в год для высокорисковых систем
- Мониторинг: отслеживание drift, точности, предвзятости
- Инциденты: процедура реагирования на сбои и ошибки ИИ

7. Обучение и осведомлённость

- Обязательное обучение для всех, кто использует ИИ
- Углублённое обучение для разработчиков и аналитиков
- Регулярные обновления при изменении политики

8. Ответственность и санкции

- Нарушение: предупреждение → обучение → дисциплинарное взыскание
- Ответственный за политику: [должность] утверждает и обновляет
- Пересмотр: не реже 1 раза в год или при изменении регулирования