Time-to-Market по закону

Риски использования AI-агентов в мобильной разработке

Иван Шевелев

Руководитель практики правового и инвестиционного обслуживания MyFilm48 Consulting

Иван Шевелев

MyFilm48 Consulting

→ Юрист

→ Преподаватель СПбГУ

→ Эксперт по IP и IT-праву

Специализация

Консультирую цифровые и ИТ-проекты

Фреймворки

Пользовательское программирование

LLM и ИИ-ассистенты

Исследования

Научный сотрудник СПбГУ. Защитил диссертацию о правовых аспектах пользовательского программирования

Что мы разберем сегодня

Три ключевые управленческие дилеммы:

01 **Скорость против безопасности**
Как ускорять TTM с помощью AI-агентов без риска реджектов в сторах

02 **Когда проверять код**
На этапе написания в IDE / Перед сборкой билда / После реализации риска

03 **Распределение ответственности**
Кто платит, если сгенерированный ИИ код нарушает чужие права

Чек-лист

Готовое решение для применения на практике в следующем спринте

→ Практические инструменты
→ Реальные кейсы
→ Действия для команды
→ Правовая база: какие законы применяются

Правовая база: какие законы применяются

Авторское право Гражданский кодекс РФ	Регулирует, кому принадлежит сгенерированный код и что значит нарушить исключительные права	→ Авторство при AI-генерации всегда у человека, не у ИИ
Data и лицензии ФЗ-152 / ФЗ-98 / FOSS	Персданные в промптах, коммерческая тайна в GPT, юридическая сила открытых лицензий	→ NDA + слив в промпт = уголовная ответственность
Ответственность КоАП / УК / EULA	За нарушение авторских прав и условий сервисов	→ Правовой вакуум — миф. Регулирование уже работает

Цена AI-ошибки для бизнеса

App Store и Google Play

Удаление приложений или бан аккаунта. Чаще блокируют за изображения/шрифты, чем за код, но при M&A именно код идет под проверку

Российские реалии

Samsung 2023: утечка кода через ChatGPT — введены тотальные ограничения. Ущерб P&L несет паблишер/заказчик

Инвестиции и M&A

Срыв сделки, занижение оценки компании, если в исходном коде приложения обнаружен "токсичный" сгенерированный код

Страхование и партнерства

Отказ в контрактах с enterprise-клиентами из-за утечек данных через ИИ-ассистентов

ОДНА ОШИБКА = МИЛЛИОНЫ ПОТЕРЬ

Скорость или безопасность?

Давление на команду

Конкуренты выкатывают фичи в два раза быстрее благодаря Codex, Claude Code и т.д.

Инвесторы и стейкхолдеры требуют сокращения сроков

Команда разработчиков уже активно и неконтролируемо использует ИИ-агентов

Риски использования AI

→ Утечка ключей API и проприетарного кода через промпты разработчиков в облако ИИ

→ Нарушение GPL/AGPL при копировании сгенерированных компонентов.
Кейс: AGPL-код в продукте срывает M&A сделку при due diligence

→ Риск удаления из стора из-за генерации ассетов, нарушающих чужой копирайт

БЫСТРО ≠ БЕЗОПАСНО

Три пути интеграции AI-агентов

Fast Track

Подход:

Быстрая генерация и деплой, минимум проверок

Главный риск:

Страйки за копирайт и баны аккаунтов постфактум

Safe Track

Подход:

Ручное ревью каждой строчки юристами
и безопасниками

Главный риск:

Релиз в 3-5 раз медленнее, кратный рост стоимости разработки (потеря сути TTM)

Risk-Based

Подход:

Правовая функция встроена в CI/CD и среду разработки

Главный риск:

Требует зрелости процессов и культуры внутри мобильной команды

Risk-Based — БАЛАНС СКОРОСТИ И БЕЗОПАСНОСТИ

Risk-Based в AI-разработке

Формы участия правовой функции

Асинхронное ревью ИИ-зависимостей и архитектуры приложения

Участие в тех. ревью при выборе разрешенных AI-инструментов для команды

Чек-поинты перед отправкой билда в TestFlight / Google Play Console

Пример анализа риска

Идентификация:
«ИИ сгенерировал модуль авторизации на базе лицензии GPL = риск заражения всего приложения»

Оценка толерантности:
«Продукт коммерческий → риск высокий, вероятность средняя»

Рекомендации:
А: Переписать модуль руками | Б: Использовать проверенный Open-Source SDK | В: Принять риск + сформировать резерв

Три модели контроля AI-кодогенерации

Secure by Design
(На каждом этапе)

Настройка корпоративных политик в IDE, отключение телеметрии и обучения ИИ

Сферы: Финтех, MedTech, Enterprise

Риск-профиль: Ошибка критична

Gate-Review
(Один раз перед релизом)

SAST-анализ и проверка лицензий перед сборкой и отправкой в стор

Сферы: Игры, E-commerce, Утилиты

Риск-профиль: Возможны баны в сторах, вред репутации

Reactive
(После запуска)

Реакция на инциденты и страйки от Apple/Google

Сферы: Внутренние инструменты, пет-проекты прототипы

Риск-профиль: Готовы к удалению продукта

Практика: ИИ, код и дизайн

Правовой статус ИИ

Суды НЕ наделяют ИИ правосубъектностью
ИИ = инструмент (как клавиатура или среда разработки)

Ответственность

Ответственность всегда на человеке (разработчике) или организации (студии)

Дело Thaler vs. Copyright Office

ИИ-ассеты (иконки, персонажи) не защищаются авторским правом без творческого вклада человека. То же — для кода

Риски кодогенерации
(Copilot / Claude Code)

ИИ-ассистент может выдать точную копию чужого проприетарного кода или кусок под вирусной лицензией

Встраивание этого кода ведет к нарушению прав третьих лиц. Важно: разработчик может не знать, что код чужой, но незнание не освобождает от ответственности

Российская судебная практика

Дело А40-200471/2023
Рефейс Технолоджис vs Бизнес-Аналитика

Deepfake-ролик использован без разрешения. Суд признал: ИИ — инструмент, автор — человек

Дело А42-3966/2023
Защита ИИ-изображения
Ответчик: ИИ создал — нет авторских прав.
Ключ: исходник — доказательство авторства

Суд признал право истца. Вывод: документируйте промпты, исходники, промежуточные версии

Позиция СИП 2024
Суд по интеллектуальным правам

ИИ-видео охраняется при творческом вкладе человека. Два условия: создан творческим трудом + выражен в некой форме

Суды последовательно применяют авторское право к AI-генерации. Документируйте процесс: промпты, исходники, техзадания — это ваша страховка и доказательство авторства

Что НЕ работает в мобайле

Типичные антипаттерны AI-комплаенса

Глухие запреты на AI
Разработчики все равно будут использовать нейросети в обход правил

Сложные корпоративные AI Policy
«too long; didn't read»

ПОЧЕМУ ЭТО НЕ РАБОТАЕТ

→ Игнорирование реальности: разработчики уже используют AI

→ Отсутствие практичности: сложные правила не применяются

→ Нет интеграции в workflow: правила существуют отдельно от процесса

→ Нет контроля: невозможно отследить использование

Решение 1: Карта рисков кодогенерации

Карта правовых рисков за 4 шага

01 Идентифицируйте

Точки риска (какие агенты используются: Codex, Claude Code, Cursor, Copilot; какие данные утекают в промпты)

02 Оцените

По матрице «Вероятность наступления × Влияние на процессы и выручку»

03 Приоритизируйте

Выделите критичные бизнес-риски

04 Назначьте

Владельца риска (например, PM или Tech Lead)

★ Матрица оценки

Вероятность:

Низкая / Средняя / Высокая

Влияние:

Низкое / Среднее / Высокое

Риск = Вероятность × Влияние

Решение 2: Встроенные процессы

Правовые чек-поинты, интегрированные в существующий workflow

01 Инициация

Асинхронные выбор и утверждение безопасных AI-инструментов

02 Выбор среды

Аудит настроек приватности; запрет на использование корпоративного кода для дообучения моделей

03 Разработка

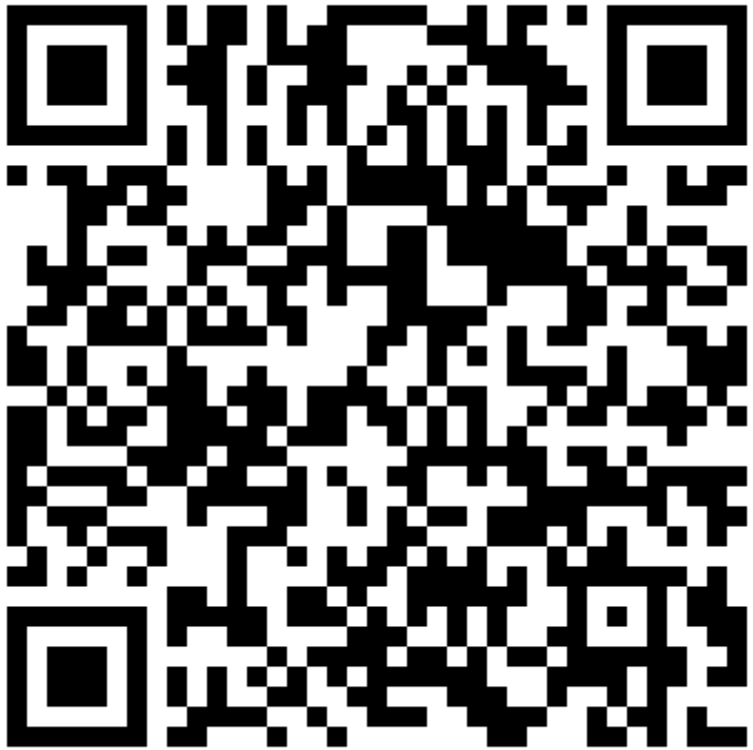
Автоматизированная проверка лицензий (SAST) + промежуточные чек-поинты

04 После релиза

Мониторинг обновлений гайдлайнов Apple/Google в отношении ИИ-контента

ПРАВОВОЙ КОМПЛАЕНС — ЧАСТЬ ПРОЦЕССА, А НЕ ПРЕПЯТСТВИЕ

ЧЕК-ЛИСТ БЕЗОПАСНОЙ РАЗРАБОТКИ



Кто в итоге заплатит за "токсичный" код?

Факт 1 Ожидание - реальность	**Ожидание**: виноват OpenAI или GitHub **Реальность**: платформы забанят аккаунт паблишера. Суд всегда взыщет с владельца продукта
Факт 2 Момент принятия решения	Критическое решение принимает не юрист в суде, а разработчик или лид в момент апрува Pull Request'а с ИИ-кодом
Факт 3 Законные последствия	Стандартные EULA не обезопасят, если ИИ скопировал чужой коммерческий SDK. Штрафы и убытки придется платить из чистой прибыли студии

ОТВЕТСТВЕННОСТЬ НЕ ПЕРЕЛОЖИШЬ НА ИИ

Личная ответственность разработчика

Наемный сотрудник
ТК РФ: лимит — 1 месячный оклад (ст. 241). Превышение только при доказанном умысле или специальной норме трудового договора

Пример: слил исходники — полная матответственность по ст. 243 ТК

ИП-разработчик
Без ограничений ТК
Отвечает всем имуществом, нет “корпоративного щита” — личные активы и бизнес-риски не разделены

Риск: претензия заказчика на полную сумму убытков без ограничений

Директор / CEO
Ст. 53.1 ГК РФ: отвечает за убытки компании при виновных действиях. Риск субсидиарной ответственности при банкротстве

Позиция судов: незнание IP-закона не освобождает от ответственности

Кто и как отвечает в AI-экосистеме

Разработчик (наемный)
Скормил закрытый код или ключи в публичный ChatGPT

Последствия: дисциплинарная ответственность, увольнение

Студия-разработчик
(Аутсорс / Продуктовая команда)
Сдала релиз с чужими датасетами или токсичным кодом от ИИ

Последствия: потеря контракта, штрафы 1x-2x от стоимости разработки

Паблишер / Заказчик
Получил страйк в App Store/Google Play за нарушение авторских прав в коде/дизайне

Последствия: удаление приложения, потеря базы, ответственность перед конечными пользователями

Что делать? Защита от рисков

ПЛАТИТ ТОТ, У КОГО ХУЖЕ ЮРИСТЫ ИЛИ КОНТРАКТЫ

01. Для студий-разработчиков (аутсорс)

→ Включайте четкие ограничения ответственности за сгенерированный ИИ контент

→ Настройте фильтрацию ИИ-ввода на уровне IDE

02. Для продуктовых компаний и паблишеров

→ In-house команды: аудит ИИ-инструментов и SAST

→ Зеркальные меры + требуйте гарантии легальности

→ Документируйте проверки (доказательство due diligence перед платформами)

03. Для всех

→ Принцип «пишите, как делаете» — фиксируйте правила использования AI письменно

→ Отключайте настройки телеметрии и обучения на ваших данных в платных подписках Copilot/ChatGPT

Что мы узнали сегодня

TTM vs. Безопасность	Risk-Based подход позволяет ускорять релизы с помощью AI, предотвращая фатальные блокировки в сторах
Когда проверять код	Выбирайте путь под риск-профиль
Кто заплатит	Российские суды применяют авторское право к AI. Платформы наказывают паблишера — распределяйте ответственность в договорах заранее
Решения, которые работают	Карта рисков + интеграция в CI/CD + чек-лист + четкие договоры с разработчиками

Инструменты: осязаемые и неосязаемые

1. Осязаемое

Чек-лист проверки ИИ-кода перед отправкой на ревью в стор

2. Неосязаемое

→ Интегрируйте правила в процессы (настройки IDE, доступы)

→ Документируйте выбор тулзов — ваша страховка перед Apple/Google

→ Распределяйте ответственность до инцидентов

Что НЕ делать:

→ НЕ игнорируйте гайдлайны платформ и Open-Source лицензии

→ НЕ полагайтесь на "это написал Copilot, я не виноват" — ни сторы, ни суды это не примут

Что делать в следующий спринт (5 шагов)

1. **Аудит реальности**
   Узнайте, какие AI-агенты уже де-факто использует ваша mobile-команда

2. **Соберите команду**
   Tech Lead (iOS/Android) + Юрист + Продакт-менеджер

3. **Настройте доступы**
   Отключите отправку корпоративного кода на обучение ИИ в корпоративных аккаунтах

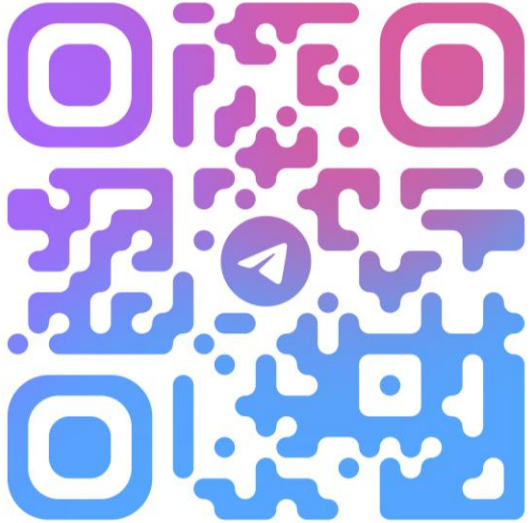
4. **Обновите пайплайн**
   Внедрите проверку лицензий сгенерированного кода перед релизными сборками

5. **Задокументируйте**
   Создайте короткий playbook (внутренний гайдлайн) по легальному использованию ИИ для разработчиков

ПРАВОВОЙ КОМПЛАЕНС НЕ РУШИТ ТТМ

ОН ЗАЩИЩАЕТ ВАШ ПРОДУКТ ОТ УДАЛЕНИЯ ИЗ СТОРОВ

Спасибо за внимание!



mail.shevelev@gmail.com

TG: @shevelevivan