PLAYBOOK · ВЕРСИЯ 3.0 · РФ

AI Adoption Audit

для российского enterprise

Пошаговый фреймворк для CIO и Chief AI Officer: как посчитать теневой AI, оценить риски с оглядкой на 152-ФЗ и санкционную реальность, собрать governance, который не развалится при первой же проверке РКН.

3.0

Илья Утов

t.me/gorilla_under_hood

База: playbook v2 (global) + BBVA case study (HBR, апрель 2026)
+ российская регуляторика + практика enterprise в условиях ограниченного доступа к western AI.

Апрель 2026

Зачем отдельный playbook для РФ

Кому: CIO, CTO, Chief AI Officer, Head of Information Security в компаниях от 500 сотрудников.
Сколько времени: 60–90 дней на полный audit, 14 дней на быстрый.

Универсальный playbook на базе BBVA годится как каркас. Но три фактора меняют расклад так, что точечные правки не спасают.

Фактор 1 · Доступ к western AI

OpenAI, Anthropic, Google не обслуживают российские юрлица с начала 2024 года. Рынок вывернулся через KZ/UAE/AM-юрлица, прокси-API, личные VPN и частные подписки. Shadow AI в РФ тянет на **60–80%** реального использования против 40–60% в global.

Фактор 2 · 152-ФЗ

Персональные данные граждан РФ хранятся на территории РФ. Точка. Прогнать ПД через зарубежный AI без локализации и согласия субъекта = нарушение автоматически. РКН штрафует с 2022-го, штрафы растут.

Фактор 3 · Местные платформы подтянулись

GigaChat (Сбер), YandexGPT, T-Lite (Т-банк), MTS AI, Cloud.ru AI к 2026-му закрывают **70–85%** типовых задач: тексты, код, поиск, суммаризация. Для чего-то хватает. Для чего-то нет — и дальше по этому нужно принимать решение.

Три фактора вместе переписывают три из пяти принципов enterprise adoption. Отсюда отдельная версия, не overlay.

Содержание

Парадокс российского shadow AI

Средний российский банк, телеком или IT-компания от 1 000 человек. Картина обычно такая.

Официально: куплен корпоративный контракт на YandexGPT или GigaChat. Пилот на 50–200 человек. Compliance одобрил. Совету директоров показали слайд про «мы внедряем AI».

Неофициально: ведущий аналитик данных сидит в ChatGPT через VPN и личную подписку. Финансовый директор получает доступ через родственника в казахстанском юрлице. Разработчики используют Claude через прокси-API, который оплачивают из общего пула «на облако». Маркетологи тащат задачи в Gemini с бытовых VPN.

> **Разрыв между «куплено» и «используется» — 5×**
>
> И весь этот shadow: без audit trail · крутит корпоративные данные, часто с ПД · принадлежит сотруднику, а не компании · уходит вместе с сотрудником при увольнении · создаёт compliance-риски по 152-ФЗ и санкционному праву · висит на личных картах.

Playbook помогает честно посчитать эту реальность и начать приводить её в порядок.

Кому это нужно прямо сейчас

- **Новый Chief AI Officer или CIO.** Первые 90 дней в роли. Совет ждёт baseline: где мы на самом деле и куда идём.
- **Проверка РКН или ФСТЭК в горизонте 6 месяцев.** Inspection попросит доказательств governance. Без audit их просто нет.
- **M&A или due diligence.** Покупатель спросит про AI-стек, compliance, технологические риски. Ответ должен опираться на цифры.

Плюс триггеры поменьше: утечка через AI-сервис (в РФ к апрелю 2026 несколько публично зафиксированных кейсов), крупная сделка с transparency-обязательствами, смена регулятора в отрасли.

5 принципов enterprise adoption в российской реальности

Пятёрка та же, что в global. Три принципа требуют специфичной подгонки под РФ: путь доступа, состав compliance-комитета и формат культурного buy-in. Остальные два (внутренний каталог и workflow-метрики) переносятся с минимальными правками.

01 Licence first, control second

Полная формулировка

Компания сначала даёт всем сотрудникам корпоративный доступ к enterprise-tier AI-инструменту, и только потом строит governance вокруг этого доступа. Логика обратная привычной ИБ-последовательности «сначала policy, потом раскатка». Причина: если официального доступа нет, сотрудники всё равно начнут использовать AI через личные каналы. Shadow AI появится быстрее, чем policy.

BBVA прошёл это на цифрах: после enterprise-контракта с OpenAI и раздачи ChatGPT Enterprise **11 000** сотрудникам shadow-использование упало в разы, потому что исчез стимул. Governance (audit logs, DLP, approval process) приходит поверх уже существующего sanctioned-контура, а не вместо него.

В РФ даже первый шаг неочевиден. На глобальном рынке enterprise-доступ значит «покупаем ChatGPT Enterprise, Claude for Work или Gemini Advanced и раздаём сотрудникам». В России это опция, которой прямым путём просто нет. «Доступ» становится переменной, которую нужно определять отдельно.

Пути, между которыми приходится выбирать

- **Локальный enterprise-контракт** с YandexGPT, GigaChat, MTS AI. Быстро, легально, 152-ФЗ решается при правильной настройке. Потолок ниже global frontier-моделей. Для 70–85% задач хватает.
- **Партнёр в KZ, UAE или AM** с перепродажей western-лицензий. Легально при аккуратном оформлении. Дороже оригинала на 30–60%. Continuity-риск: поставщик может отвалиться в любой момент.
- **Прокси-API** через российских агрегаторов. Доступ к GPT, Claude, Gemini через их оптовые контракты. Серая зона: sanctions-нарушение на стороне vendor, но не прямая коллизия с РФ-законом. Юридический комфорт средний, ответ зависит от вашего юриста.
- **Свой фронт к open-source** (Llama, Qwen, Mistral, Saiga, T-Lite). Self-hosted или в Yandex Cloud, Cloud.ru, VK Cloud. Полный контроль над данными. Цена: DevOps и ML-инженер в штате.

Честный вопрос себе

Компания определилась, каким путём даёт сотрудникам доступ? Если ответа нет, сотрудники выбирают сами. И **80% выбирают путь, который компания контролировать не сможет**.

02 Внутренний каталог кастомизаций

Суть принципа

Enterprise adoption работает только тогда, когда ценные AI-workflows превращаются в актив компании, а не остаются в голове отдельных сотрудников. BBVA построил **4 800 custom GPTs** на 11 000 сотрудников именно так: каждый pipeline документируется в виде манифеста, проходит approval, публикуется во внутреннем каталоге и используется коллегами.

Компоненты минимальной реализации: единый формат манифеста, approval-процесс, usage-телеметрия, квартальный review. Без каталога каждый сотрудник переизобретает колесо, а при увольнении уносит всё с собой.

РФ-специфика одна, но важная. Каталог редко строится на одной платформе. GigaChat плюс YandexGPT плюс прокси-API к Claude плюс self-hosted Llama для чувствительных данных — это нормальная конфигурация российского enterprise. Отсюда требование: формат манифеста platform-agnostic. Workflow описан через «функция + промпт-схема + требования к модели», а не через «скрипт под конкретный endpoint». Это стоит дороже на старте, но окупается первым же переносом.

Почему в РФ это критичнее, чем в global. Зарубежный vendor может уйти за 30 дней — OpenAI показал это в январе 2024-го. Партнёрские каналы в KZ периодически теряют доступ к upstream. Каталог с переносимыми манифестами превращается из витрины в страховой полис.

Вопрос на проверку

Если завтра компания потеряет доступ к основному AI-vendor, сколько workflows останутся работоспособными без переписывания с нуля? Меньше 50% = каталог страхует плохо.

03 Compliance с нулевого дня

Формулировка принципа

Legal, security и risk заходят в AI-проект на этапе дизайна, не после первого rollout. Shift-left: compliance встроен в архитектуру, а не прикручен сбоку постфактум.

В global-практике это присутствие privacy officer, security architect и risk manager на планёрках продукта, ревью данных перед обучением/файн-тюнингом моделей, ownership каждого AI use case, AI ethics review для customer-facing систем.

В РФ состав участников шире. Четыре роли должны сидеть в комитете одновременно, не по очереди.

Юрист по 152-ФЗ	Определяет, какие данные через какой путь доступа можно обрабатывать, готовит согласия субъектов, отвечает за Data Localization Statement.
Специалист ИБ с ФСТЭК	Обязателен для компаний с гостайной или КИИ (187-ФЗ). Threat modeling, выбор технических controls.
Risk officer	Оценивает санкционные риски конкретного пути (прокси-API, партнёрские схемы KZ/UAE/AM), моделирует сценарии отзыва лицензий.
Compliance officer	Мониторит регуляторную динамику. 2025–2026 активно обсуждают сертификацию критичных AI-систем, формулировки меняются.

Фраза, от которой должно сводить зубы

«У нас разработают AI Acceptable Use Policy после пилота.» В РФ это особенно плохо. Пилот обработает ПД через shadow-канал, первый инцидент создаст нарушение, и policy задним числом его не закроет.

04 Лидеры обучаются первыми

Что это значит

Top-команда (CEO, совет директоров, C-level) проходит AI-обучение раньше и глубже, чем линейные сотрудники. Не лекцию на вебинаре, а реальное обучение: 10+ часов, с практикой, с работой над собственными задачами руководителя, с разбором кейсов.

В BBVA председатель и CEO сделали это публично: на Workshop в мае 2024-го показали, как используют GPT для подготовки к заседаниям совета. Эффект: линейные руководители перестают блокировать использование AI подчинёнными, потому что их собственный босс делает то же самое.

В РФ этот принцип работает жёстче, причина культурная. Top-down культура в среднем российском enterprise выражена сильнее, чем в F500. Без явного buy-in CEO и совета линейный руководитель скажет подчинённому: «не трать на это рабочее время». AI-инициатива умрёт раньше, чем начнётся. Паттерн задокументирован в исследованиях McKinsey Russia до 2022-го и СберИнсайт 2024–2025.

Рабочий критерий выполнения

CEO и председатель совета прошли полноценное обучение (10+ часов, с практикой, с разбором рабочих кейсов). Двухчасовой брифинг от подрядчика не считается.

Индикатор

На встрече топ-менеджмента кто-то показывает решение, собранное через AI. Реакция совета ближе к «покажи как ты это сделал» или к «мы тут серьёзные вопросы обсуждаем»? Ответ = уровень buy-in.

05 Workflow metrics, не seat metrics

Seat metrics врут везде.

Принцип полностью

Традиционный способ отчитываться о AI-adoption — «у нас куплено N лицензий / активировано M сотрудников». Это vanity metric: показывает, что бюджет освоен, но не показывает, что компания получила.

Правильные метрики смотрят на workflows: сколько рабочих процессов переведено на AI, сколько часов в неделю сэкономлено, какое качество output (ниже rework rate, выше customer CSAT), как растёт каталог плагинов, как быстро workflows проходят approval.

РФ-нюанс. В России seat metrics врут сильнее, чем в global, по простой арифметике. Если реальное использование в 5 раз выше официального (типичное РФ-соотношение), отчёт «у нас 200 sanctioned seats» занижает картину в те же 5 раз. Вы показываете совету цифру, по которой нельзя принять ни одного решения: ни про инвестиции, ни про ограничения, ни про обучение.

Выход — не перестать считать seats. Считайте. Но дополните второй метрикой, «реальное использование», через ежеквартальный анонимный опрос. Рядом положите workflow-показатели: сколько плагинов в каталоге, сколько активно используются, сколько часов в неделю сэкономили power users.

Проверка

Сколько сотрудников использует AI еженедельно по последнему анонимному опросу? Если эта цифра больше sanctioned seats в 2+ раза, workflow metrics нужны срочно, не в следующем году.

Диагностический чеклист перед audit

Прежде чем запускать audit, прогоните компанию по 7 вопросам. Y/N с обязательным evidence.

#	Вопрос	Если N, первый шаг
01	Путь доступа определён (локальный / партнёр / прокси / open-source)	Решение через совет, зафиксировать в AI-стратегии
02	Внутренний каталог workflows существует (хотя бы Notion-страница)	Собрать топ-20 промптов от power users в одно место
03	Юрист по 152-ФЗ одобрил путь обработки ПД	Встреча в Q + 30 дней
04	Специалист ИБ провёл threat modeling	Включить ИБ в governance committee
05	CEO и правление прошли обучение 10+ часов	2-дневный intensive в Q + 60 дней
06	Метрика adoption показывает workflows, не seats	Заменить dashboard на workflow counter
07	Анонимный опрос по реальному использованию проведён	Survey в Q + 14 дней

Как читать результат

- **7 из 7** · Редкость. Вы в топ-5% российских компаний по зрелости AI-adoption.
- **5–6 из 7** · Хорошая база. Audit добивает остаточные пробелы.
- **3–4 из 7** · Типичная РФ-картина. Audit критичен.
- **0–2 из 7** · Компания живёт на shadow AI. Audit обязателен, стартуйте с Phase 1.

Как читать 7 пунктов вместе

Первые три пункта — compliance. Следующие четыре — здоровье внедрения. Провал в первых трёх грозит штрафом. Провал в остальных грозит тем, что adoption просто не случится, сколько бы лицензий вы ни купили.

Структура audit: 5 фаз

#	Фаза	Срок	Что делаем	РФ-акцент
01	**Discovery**	дни 1–14	Полная инвентаризация	Включая shadow-каналы и personal VPN-подписки
02	**Classification**	дни 14–28	Категоризация по use case, риску, compliance	Добавить ось «путь доступа» и «152-ФЗ совместимость»
03	**Risk Assessment**	дни 28–45	Top 10 зон внимания	Приоритет: обработка ПД через зарубежный AI
04	**Structure & Governance**	дни 45–70	Policy, catalog, technical controls	Выбор legal path, локализация данных
05	**Continuous Monitoring**	70–90 и далее	Operational cadence	Квартальный мониторинг регуляторики

P1 Discovery · дни 1–14

Задача: увидеть все AI-инструменты, которые реально в работе. В РФ 60–80% обнаруженного не окажется ни в одной официальной закупке.

1.1. Выгрузка из billing и expense reports

Финотдел вытаскивает extract за последние 12 месяцев. Что ищем:

- Подписки на российские AI (GigaChat, YandexGPT, MTS AI, Cloud.ru)
- Зарубежные подписки через KZ/UAE/AM-юрлица, если такие есть
- Expense reports со словами AI, GPT, Claude, Gemini, OpenAI, Anthropic, ChatGPT, Midjourney, Perplexity
- API-расходы через Yandex Cloud, Cloud.ru, VK Cloud, MTS Cloud
- API-расходы через российских прокси-агрегаторов
- Vendor-AI-features в SaaS (CRM, HR-системы, 1С с AI-модулями)

> **Нюанс**
>
> Часть сотрудников платит за AI из личных денег и не компенсирует через expense. Billing не увидит **40–60%** реального использования. Это закрывает следующий шаг.

Output. Таблица: вендор × путь доступа × тип лицензии × seats × стоимость за год × отдел.

1.2. Анонимный опрос сотрудников

Критично для РФ. Billing слеп к большей части реальности. Шесть вопросов:

1. Какие AI-инструменты вы используете в работе (список + «другое»)?
2. Как часто (ежедневно / еженедельно / реже)?
3. Кто платит за подписку (компания / лично)?
4. Если лично: какая сумма в месяц?
5. Через какой канал: корпоративная лицензия / VPN + личная карта / прокси-API / партнёр в другой стране / не знаю?
6. Знаете ли вы корпоративные правила по AI (да / нет / есть, но непонятные)?

> **Главное для respond rate**
>
> Анонимность + письменное обязательство топ-менеджмента «никаких санкций за любой ответ». Без этого в РФ respond rate падает до 10–15% из-за страха дисциплинарных мер за shadow-использование. Ожидаемый respond rate при правильной подаче: **35–55%**.

1.3. Technical discovery

IT и security делают несколько вещей параллельно.

- **DNS-логи.** Запросы к OpenAI, Anthropic, Cohere, Google AI, а также к известным прокси-агрегаторам.
- **Browser extension audit.** Chrome и Edge в корпоративной среде: какие AI-расширения стоят.
- **Corporate-installed apps.** Плюс iOS/Android MDM-профили.
- **Network traffic analysis** через CASB или DLP для AI-доменов.

> **Специфика РФ**
>
> В global technical discovery ловит порядка **80%** shadow AI. В РФ ловит **30–50%** из-за VPN и личных устройств. Survey и интервью power users закрывают остальное.

1.4. Интервью с power users

Выделите 20–30 «power users» из survey. 30-минутные интервью. Вопросы специфичные для РФ:

- Какие задачи решаете через AI?
- Через какие платформы (российские / зарубежные / смешанно)?
- Если зарубежные: как получаете доступ? Насколько стабильно?
- Что бы использовали при корпоративном доступе?
- Какие workflows построили? Передаёте коллегам?
- Что бесит в текущей ситуации?

Побочная цель: понять, какая часть shadow AI перейдёт в корпоративный контур, если компания предложит легальную альтернативу. Не все переходят, и это надо знать заранее.

> **Phase 1 Deliverable · AI Adoption Baseline**
>
> Один документ, восемь цифр: total corporate spend (₽) · estimated personal spend (₽) · total sanctioned users · estimated total real users · shadow-to-sanctioned ratio · top 10 tools by usage (русские/зарубежные отдельно) · top 10 tools by spend · coverage (% сотрудников, использующих AI хотя бы еженедельно).
>
> Документ идёт совету с одним тезисом: **вот разрыв между тем, что мы покупаем, и тем, что реально происходит**.

P2 Classification · дни 14–28

Задача: категоризировать обнаруженное по четырём осям.

2.1. По use case

Для каждого workflow фиксируем:

- **Функция:** code / writing / analysis / research / automation / customer-facing / decision support
- **Данные:** public / internal / confidential / PII (граждан РФ) / финансовые / health / гостайна
- **Отдел-владелец:** кто использует больше всего

2.2. По риску

Матрица 4×4: impact (low / med / high / critical) × likelihood (rare / occasional / frequent / constant). Impact по четырём факторам, подогнанным под РФ:

- **Regulatory exposure.** 152-ФЗ, 187-ФЗ о КИИ, ФЗ-149, требования ФСТЭК, отраслевые регламенты.
- **Financial exposure.** Штрафы РКН (до 18 млн ₽ за нарушение приземления на юрлицо, 2024 г.), претензии клиентов.
- **Reputational exposure.** Публикация в СМИ о shadow AI, утечка данных через AI-сервис.
- **Operational exposure.** Зависимость core business от платформы, которая может уйти с рынка.

2.3. По compliance tier

В РФ tier'ов четыре, не три, как в global.

Tier 1 · Compliant	Корпоративный контракт с российским vendor. Локализация ПД подтверждена. Аудит-логи доступны. 152-ФЗ закрыт.
Tier 2 · Borderline	Контракт с зарубежным vendor через легальный KZ/UAE/AM-канал. ПД обрабатываются, но вопрос приземления решается отдельно. Юрист проверяет.
Tier 3 · Grey	Прокси-API или корпоративный VPN на зарубежный сервис. Серая зона: sanctions-нарушение на стороне vendor, но не прямая коллизия с РФ-законом. Нужен risk assessment.
Tier 4 · Shadow	Personal-tier сервис, оплачен лично, без корпоративного контракта. С корпоративными данными. Audit trail отсутствует. ПД граждан РФ едут за пределы РФ без согласия субъекта = нарушение 152-ФЗ.

2.4. По legal path

Новая ось, только для РФ. Каждый инструмент получает одну метку:

- локальный vendor
- партнёр в другой стране (с договором)
- прокси-API (с договором)
- VPN + личная подписка
- неизвестно

> **Phase 2 Deliverable**
>
> Matrix «Tool × Use case × Risk level × Compliance tier × Legal path». Визуализирует реальное положение compliance и задаёт приоритеты для Phase 3.

P3 Risk Assessment · дни 28–45

Задача: приоритизировать и достать Top 10 зон.

3.1. Автоматические красные зоны

В РФ в красную зону автоматом попадают четыре пересечения.

Red zones

- **Tier 4 Shadow + обработка ПД граждан РФ.** Прямое нарушение 152-ФЗ. Immediate action.
- **Tier 3 Grey + frequent/constant use.** Санкционный и операционный риск. High priority.
- **Tier 2 Borderline + финансовые данные.** Возможные претензии Банка России или финрегуляторов.
- **Любой tier + данные КИИ.** 187-ФЗ, требования ФСТЭК. Отдельный режим оценки.

Ожидаемое количество: 8–20 кейсов в компании 500–5 000 сотрудников. В РФ обычно ближе к верхней границе из-за преобладания shadow AI.

3.2. Pre-mortem каждой красной зоны

Для каждой зоны: «если завтра этот workflow утечёт, ошибётся или попадёт под проверку РКН, что будет?» Фиксируем:

- вероятность (1–10)
- штраф или претензия (₽)
- репутационный ущерб (шкала)
- время восстановления
- detect'ability: кто и как заметит

Специфика РФ

Добавьте сценарий «регулятор пришёл с проверкой завтра». Для shadow AI с обработкой ПД это вопрос времени, не гипотетика. В 2024–2025 РКН провёл целевые проверки именно по shadow AI в крупных компаниях.

3.3. Gap analysis

Сравните состояние компании с:

- **NIST AI Risk Management Framework.** Универсальный бенчмарк.
- **ISO 42001.** AI management system, сертификация доступна в РФ через аккредитованные центры.

- **Рекомендации Банка России** по управлению рисками AI в банковском секторе, 2024–2025.
- **Проект AI-закона РФ.** На апрель 2026 в разных стадиях обсуждения, сверяйтесь с материалами Минцифры.
- **BBVA case study.** Внешний бенчмарк лучшей практики.

> **Phase 3 Deliverable**
>
> Report «Top 10 AI Risks» с конкретными сценариями, оценками и предлагаемыми mitigations. Документ для совета с явным разделением: что требует immediate action и что откладываем на Phase 4.

P4 Structure & Governance · дни 45–70

Задача: собрать систему, которая устоит перед регулятором и операционными шоками.

4.1. Шесть вопросов совету директоров

В global-версии было пять. В РФ добавляется шестой, о пути доступа.

1. **Путь доступа.** Локальный vendor / партнёр в другой стране / прокси / hybrid. Каждый путь разный по стоимости, compliance и continuity.
2. **Какой enterprise-tier покупаем и для кого.** GigaChat для всех, YandexGPT для выбранных отделов, прокси-API к Claude для инженерии, open-source self-hosted для данных КИИ.
3. **Кто отвечает за governance.** Существующая роль (CIO, CISO, compliance officer) или новая Chief AI Officer.
4. **Risk appetite.** Conservative (только Tier 1), balanced (Tier 1 + аккуратный Tier 2), aggressive (Tier 3 разрешён под контролем).
5. **Что prohibited.** Обработка ПД клиентов через Tier 3–4. Данные КИИ через любой зарубежный сервис. Automated customer communication без review.
6. **Как измеряем успех.** Workflow metrics, не seat metrics. С учётом shadow-части через ежеквартальный анонимный опрос.

4.2. Internal AI catalog

На основе найденного собираем internal catalog workflows. Минимальный состав:

- Plugin manifest format, platform-agnostic, чтобы переносить workflows между vendors
- Approval workflow: security + юрист по 152-ФЗ + бизнес-owner
- Usage telemetry
- Quarterly review process

4.3. Policy documents

В global-версии четыре документа. В РФ шесть, плюс два локальных.

AI Acceptable Use Policy	Что можно, что нельзя, с какими данными, через какие каналы.
AI Vendor Procurement Process	Как одобряется новый AI-инструмент. Обязательные чеки на 152-ФЗ и на sanctions.
AI Incident Response Plan	Что делать при утечке через AI, при проверке РКН, при внезапном отзыве сервиса vendor'ом.
AI Training Requirements	Обязательный onboarding для сотрудников с разделом про ПД.
Personal AI Usage Policy · РФ	Что сотрудник может делать с личной подпиской на рабочем устройстве. Прямой запрет на корпоративные данные.
Data Localization Statement · РФ	Какие данные обрабатываются на какой территории, через какой vendor. Документ для РКН при проверке.

4.4. Technical controls

- SSO/OAuth для всех sanctioned AI-tools
- DLP на уровне корпоративной сети для AI-доменов
- API rate limits и spend alerts
- Audit logging для всех AI-вызовов с sensitive data
- Блокировка известных прокси-доменов (или whitelist одобренных) через корпоративный firewall
- Мониторинг уплат по корпоративным картам с фильтром по AI-vendors

> **Phase 4 Deliverable**
>
> Governance package: policies + catalog + technical controls + выбранный путь доступа. Approved советом директоров. Явный sign-off от юриста по 152-ФЗ.

P5 Continuous Monitoring · 70–90 и далее

Задача: держать систему живой. В РФ регуляторика и доступность сервисов шевелятся быстро, поэтому пропускать нельзя.

5.1. Quarterly review cadence

Каждый квартал AI governance committee прогоняет чеклист:

- spend review (тренды vs budget)
- adoption metrics (workflows, не seats)
- incident log (что случилось, что извлекли)
- catalog health (новые плагины, deprecated, migration needs)
- emerging risks (новые vendors, новые use cases)
- **регуляторные изменения.** Новые приказы Минцифры, РКН, ФСТЭК. Любое изменение в формулировках 152-ФЗ.
- **vendor availability.** Есть ли риск, что основной vendor уйдёт с рынка? Готов ли backup-план?

5.2. Annual re-audit

Раз в год повторяем Phase 1 Discovery в сокращённом формате. Смотрим, насколько shadow AI вернулся.

> **Маленькая радость**
>
> В РФ shadow AI возвращается особенно охотно, если корпоративный доступ дал сотрудникам меньше, чем им хотелось. Типичное значение возврата: **30–50%** от baseline. Это выше глобального, учитывайте.

5.3. Training & culture

Четыре ритуала:

- квартальные brownbag-sessions по AI best practices
- onboarding-module для новых сотрудников с акцентом на 152-ФЗ
- public recognition для сотрудников, создавших ценные catalog entries
- newsletter с обновлениями по tools, policies и регулированию

> **Phase 5 Deliverable**
>
> Живая operational cadence. AI governance работает как часть регулярной модели, а не разовый проект.

Quick audit · 14 дней

Если 60–90 дней недоступны, вот минимальный путь.

Неделя 1

- **День 1–2:** billing extract + expense report extract
- **День 3–5:** анонимный survey с явным «no-penalty» promise
- **День 6–7:** интервью 5 power users + краткий DNS-log audit

Неделя 2

- **День 8–9:** classification по 4 tier'ам и 5 legal paths
- **День 10–11:** shortlist красных зон (фокус на обработке ПД через Tier 3–4)
- **День 12–13:** встреча с юристом по 152-ФЗ + CISO, предварительные рекомендации
- **День 14:** 1-страничный report для CEO/CFO с тремя цифрами (sanctioned spend, estimated total spend, risk count) и одним решением

Что делает Quick audit

Quick audit не заменяет полный. Он решает бинарный вопрос: **начинаем полный audit или статус-кво приемлем**. В 7 из 10 случаев результат quick audit убеждает совет начать полный.

KPIs для РФ

Семь метрик вместо шести в global. Добавлена compliance localization.

Метрика	Что измеряет	Цель
Coverage	% сотрудников под governance framework	95%+ / 6 мес
Compliance tier shift	% shadow-инструментов, перешедших в sanctioned	80%+ / 12 мес
152-ФЗ localization	% обработки ПД на локализованных сервисах	100% для ПД РФ
Incident rate	AI-инциденты в квартал	Снижение YoY
Catalog velocity	Новые approved плагины в квартал	Стабильный рост
Time-to-approve	От подачи до merge в catalog	< 10 дней
Spend efficiency	Cost per active user	Оптимизация

152-ФЗ localization — не среднее

Для ПД граждан РФ цель **100%**, не 95%. Один необработанный случай = потенциальный штраф РКН.

Три риска, которые в РФ регулярно недооценивают

R1 Vendor disappearance

Зарубежный vendor (прямой или через партнёра) может прекратить обслуживание в любой момент. Прецеденты: OpenAI заблокировал аккаунты с российскими платежами в январе 2024, партнёры в KZ периодически теряют доступ к upstream-сервисам.

Mitigation

Backup-путь для каждого критичного workflow. Локальный vendor как primary для core business, зарубежный как дополнение. Каталог с platform-agnostic манифестами.

R2 Regulatory tightening

Российское AI-регулирование в активной фазе. В 2025–2026 обсуждают обязательную сертификацию критичных AI-систем, ужесточение локализации, запреты на отдельные use cases (автоматические кредитные решения, например).

Mitigation

Quarterly review регуляторных изменений. В governance committee обязательно compliance officer. Flexibility в архитектуре, чтобы при изменении требований не переделывать всё.

R3 Personal-to-corporate migration failure

Многие ценные workflows живут на личных подписках. При переносе в корпоративный контур часть теряется: сотрудник уходит и ничего не передаёт; локальный vendor не поддерживает нужную функцию; процесс миграции сложный. Итог: компания тратит средства на governance и теряет значительную часть реальной ценности.

Mitigation

В Phase 1.4 (интервью power users) явно обсуждайте, какие workflows переносимы на локальный vendor. В Phase 4.2 (catalog) делайте onboarding для личных workflows с каким-то стимулированием, хоть публичным признанием. Сотрудники, которые делятся, должны видеть, что это ценится.

Главный тезис для российской компании

> AI adoption в РФ в 2026-м — это не проект внедрения. Это тест на способность компании работать одновременно под **ограниченным доступом**, **нарастающей регуляторикой** и **высоким shadow-использованием**.

Компания, которая считает, что всё под контролем на основе купленной лицензии GigaChat на 100 сотрудников, живёт в параллельной реальности. Реальная картина: те же 100 **плюс** 400–800 человек через VPN и личные карты, плюс эпизодические пользователи, плюс shadow data flow, плюс регулятор, который в любой момент может прийти с вопросами.

> **Вопрос совету директоров на ближайшую встречу**
>
> Мы измеряем AI-adoption по тому, что купили? Или по тому, что сотрудники реально делают, и насколько это ложится в 152-ФЗ, санкционное право и будущее регулирование?

Честный ответ определяет, проходим ли мы следующие 24 месяца. Или попадаем в СМИ по нехорошему поводу.

Что дальше?

Этот playbook — каркас. Следующая версия (3.1) добавит:

1. Survey template с РФ-формулировками
2. Risk assessment matrix с РФ-штрафами
3. Policy document templates (AI AUP, Data Localization Statement)
4. Technical controls checklist с DLP-правилами под российские сети
5. Industry-specific overlays: банки, телеком, страхование, госсектор
6. Библиотека прецедентов: штрафы РКН по AI-инцидентам

Подписывайтесь:

t.me/gorilla_under_hood

Илья Утов, апрель 2026
Telegram: t.me/gorilla_under_hood
База: playbook v2 (global) + BBVA HBR case (апрель 2026)
+ российская регуляторика