

ЧУЖИЕ СЕКРЕТЫ В СВОЕЙ ГОЛОВЕ

Что на самом деле защищает NDA



Шесть частей о границе между чужим секретом и собственной компетенцией: мировая практика, российские суды, условия договора и что меняется, когда в проекте появляется искусственный интеллект.

Александр Дублин

АНАЛИТИК БИЗНЕСА, КОНСУЛЬТАНТ, МЕНТОР



Александр Борисович Дублин

АНАЛИТИК БИЗНЕСА, КОНСУЛЬТАНТ, МЕНТОР

Я помогаю собственникам разобраться, что на самом деле происходит в бизнесе, и превратить хаос ежедневных решений в понятную систему цифр, процессов и действий.

Моя работа — это не про красивые презентации и общие советы. Я вхожу в реальную ситуацию бизнеса: смотрю управленческий учёт, продажи, процессы, клиентский опыт, роли и точки напряжения. Помогаю увидеть, где теряются деньги, почему решения буксуют и что нужно изменить, чтобы бизнес стал управляемее.

Последние 10 лет я глубоко работаю с мебельным бизнесом: продажи, производство, CRM, управленческий учёт, сервис, партнёрства, рост и кризисы. Но мой подход шире одной отрасли: я работаю с бизнесом как с системой.

Ко мне обращаются, когда собственнику нужен спокойный внешний партнёр: подумать, разобрать сложную ситуацию, собрать модель, проверить гипотезы и довести решения до внедрения.

С ЧЕМ ПОМОГАЮ

- управленческий учёт и модель бизнеса
- продажи и клиентский опыт
- процессы и правила работы
- бизнес-анализ и диагностика
- менторинг собственника
- подготовка управленческих решений

Я не занимаюсь подбором персонала и не управляю командой вместо собственника. Моя задача — помочь увидеть систему, принять решения и сделать бизнес понятнее, устойчивее и управляемее.

СВЯЗАТЬСЯ

+7 921 751-59-28

Телефон, WhatsApp · Telegram на этом номере нет

WhatsApp

написать на этот номер

Telegram @AleksandrBorisovich73

личные сообщения

ЧИТАТЬ И СМОТРЕТЬ

Telegram-канал @ab_dublin

статьи и материалы

Telegram-канал @friday_meb

пятничные посты для собственников мебельных фабрик

Дзен · dzen.ru/dbs_dubas

«Филистер филистерам. Записки антрополога бизнеса»

YouTube

«Филистер филистерам | Александр Борисович»

RUTUBE

«Александр Борисович Дублин | Системный бизнес»

ВКонтакте и VK Видео · @ab.dublin

«Александр Борисович Дублин | Системный бизнес»

Книги на Литресе

«Мебельщикам в кризис», «Мебель и коньяк», «Склад незавершёнки» и другие

Чужие секреты в своей голове

ПЕРЕД ЧТЕНИЕМ	Кому и зачем читать	2
ЧАСТЬ 1	Можно ли запретить консультанту становиться умнее?	3
ЧАСТЬ 2	Как мир делит секреты и человеческую память	9
ЧАСТЬ 3	Российский NDA: три этажа защиты и одна лестница доказательств	17
ЧАСТЬ 4	NDA как технология доверия, а не операция по удалению памяти	29
ЧАСТЬ 5	NDA и ИИ: третий в комнате	39
ЧАСТЬ 6	Разрешить, но с условиями: как консультанту работать с ИИ под NDA	46
ПОСЛЕ ЧТЕНИЯ	Где читать и смотреть дальше	54

Ссылки на законы, судебные акты и исследования в тексте кликабельны.

Кому и зачем читать

Вы показали консультанту цифры, клиентскую базу и таблицу, которую финансовый директор с гордостью называет моделью. Перед этим оба подписали NDA и успокоились. Через год консультант задаёт вашему конкуренту подозрительно правильные вопросы, хотя документов не выносил и базу никому не продавал. Нарушил он что-нибудь?

Эта статья о том, что на самом деле защищает NDA и чего он не защитит ни при каком размере штрафа. Она длинная: шесть частей, около полутора часов чтения. Поэтому сначала о том, кому она пригодится и с какой части начинать.

Владельцу бизнеса она покажет, почему фраза «вся информация конфиденциальна» в суде почти ничего не стоит, что нужно сделать до того, как открыть данные подрядчику, и как доказывать не только разглашение, но и использование ваших сведений. И отдельно о том, куда уходят ваши цифры, когда консультант загружает их в ChatGPT или Claude, и что об этом написать в договоре.

Консультанту она поможет понять, где кончается ваш опыт и начинается чужой секрет, что вы вправе унести из проекта и почему слишком широкий NDA незаметно превращается в запрет на профессию. А ещё как работать с ИИ на данных клиента и не повторить историю Deloitte, которой пришлось вернуть часть денег за отчёт с выдуманными ссылками.

Пересказа закона общими словами здесь почти нет. Зато есть номера дел, суммы и ссылки на первоисточники: как компания отсудила штраф за одно чужое коммерческое предложение, отправленное её клиенту, почему производитель вакцины проиграл спор о технологии, которая явно стоила денег, и почему суд признал законным увольнение директора по продажам, которая среди прочего выгружала отчёты компании в DeepSeek.

С чего начать, если времени мало:

- Десять минут найдутся у всех: первая часть ставит главный вопрос и раскладывает один секрет на пять состояний, от файла до навыка.
- Если скоро подписывать NDA или договор с подрядчиком, откройте четвёртую часть (18 минут), там о том, что записать и чего записывать не стоит.
- Если вы или ваш консультант работаете с нейросетями на данных клиента, вам пятая и шестая (около 27 минут).
- Суды, доказательства и номера дел собраны в третьей части (21 минута).
- Как ту же границу проводят в США, Европе и Британии, рассказывает вторая (15 минут).

Можно не читать, если вы никому не открываете внутренние данные и сами не работаете с чужими. Статья не заменяет юриста, но после неё разговор с юристом о вашем NDA станет короче и заметно предметнее.



ЧАСТЬ 1 ИЗ 6

Можно ли запретить консультанту становиться умнее?

В компанию приходит консультант. Не обязательно великий, но достаточно опытный, чтобы задавать неприятные вопросы и замечать то, к чему сотрудники давно привыкли. Ему показывают управленческую отчётность, клиентскую базу, экономику продукта, систему мотивации, внутренние конфликты и таблицу, которую финансовый директор называет «моделью», хотя при ближайшем рассмотрении это слегка одомашненный Excel-монстр.

Перед началом работы стороны подписывают NDA, соглашение о неразглашении конфиденциальной информации. Компания успокаивается: секреты защищены. Консультант тоже спокоен, потому что документ стандартный, таких он подписал десятки, а продавать базу клиентов конкурентам всё равно не собирается.

Проект заканчивается, и консультант уходит уже не тем человеком, которым пришёл. Он увидел, как устроена компания, проверил несколько гипотез, понял, какие решения работают, а какие только красиво смотрятся на презентации. Возможно, он сам помог перестроить планирование, пересобрать ассортиментную матрицу или сократить производственный цикл.

Через год он приходит к другому клиенту из той же отрасли и говорит:

— В компаниях такого типа проблема обычно не в продажах, а в том, как планируют производство. Давайте сначала посмотрим туда.

Прежнего клиента он не называет, документов не показывает, баз, чертежей, цен и паролей не передаёт и даже закрытые совещания не пересказывает. Он просто знает, куда смотреть и какие вопросы задавать.

Нарушил ли он NDA?

Владелец первой компании ответит, что конечно нарушил: знания-то консультант получил у него. Консультант ответит, что конечно нет: он никому ничего не разгласил, а думать после проекта договор ему не запрещает. Оба ответа слишком просты.

Человек уносит не только информацию

В деловой речи «информация», «знание», «опыт», «методика» и «компетенция» часто звучат как синонимы. Для разговора за кофе этого хватает, для договора и суда уже нет.

Допустим, консультант получил от клиента файл с расчётом себестоимости. Файл можно скопировать, отправить, найти у конкурента и положить на стол судье. Изучив его, консультант заметил, что компания неверно распределяет постоянные расходы, и это уже не файл, а вывод.

Потом он понял, что такая ошибка встречается у многих компаний с широким ассортиментом и неровной загрузкой производства, и получилось обобщение. А через несколько проектов он научился находить эту ошибку за двадцать минут разговора с собственником, и это уже профессиональный навык.

Причинная связь между исходным файлом и навыком есть. Простой границы, где кончается собственность клиента и начинается квалификация консультанта, нет.

Здесь и заканчивается бытовое представление о NDA как о юридическом сейфе. Сейф хорошо хранит документы, формулы, чертежи, списки клиентов, пароли и конкретные управленческие решения. Гораздо хуже он справляется с тем, что прошло через чужую голову, смешалось с прежним опытом и стало новым пониманием.

Вынести из офиса сервер под мышкой и унести из проекта мысль в голове совсем не одно и то же, хотя владельцу сервера иногда кажется, что голова теперь тоже принадлежит ему.

Разглашение и использование

Большинство российских NDA построено вокруг глаголов «передавать», «сообщать», «раскрывать» и «публиковать», то есть запрещает распространять сведения среди третьих лиц. Но чужое преимущество можно присвоить, ничего не разглашая.

Консультант узнал о ещё не объявленной стратегии выхода клиента в новый регион, никому о ней не рассказал, но помог другому заказчику выйти туда на месяц раньше. Или увидел систему ценообразования, формулу конкуренту не передал, а сам посчитал ему цены по той же логике.

Или изучил внутреннюю методику поиска перспективных территорий и применил её у другого участника рынка. Информация осталась неразглашённой, а её экономической ценностью воспользовался посторонний.

Поэтому развитые правовые системы различают раскрытие и использование коммерческой тайны. Российское право тоже: обладатель секрета производства (ноу-хау) контролирует не только передачу сведений, но и их применение, если сведения действительно отвечают признакам ноу-хау.

Нарушителем закон прямо называет, в частности, того, кто неправомерно получил такие сведения и «разгласил или использовал» их. [Статьи 1466 и 1472 ГК РФ](#)

Запрет на использование можно записать и прямо в договоре. [Статья 421 ГК РФ](#) А на стадии переговоров закон сам обязывает не раскрывать сведения, переданные как конфиденциальные, и не использовать их ненадлежащим образом для своих целей, даже если договор так и не заключат. [Пункт 4 статьи 434.1 ГК РФ](#)

Трудности начинаются не с вопроса, можно ли написать такой запрет. Написать можно многое, бумага вообще отличается высокой психологической устойчивостью. Трудности начинаются с трёх других вопросов. Что именно было запрещено использовать? Как доказать, что человек применил полученную информацию, а не собственный опыт, общедоступные знания или решение, найденное независимо?

И где заканчивается охраняемый секрет и начинается право специалиста заниматься своей профессией? Чем дальше от скопированного документа и чем ближе к усвоенному знанию, тем менее уверенно звучат ответы.

Знакомый юрист провёл эту границу одной фразой: если чужой кейс вдохновил вас на собственную идею, это ваша идея, а если вы повторили чужую идею у другого клиента, это уже очень спорно. Тем более если повторённая логика была для первой компании ценным секретом, который она охраняла. К этой границе мы ещё вернёмся.

Пять состояний одного секрета

За время проекта одна и та же информация может несколько раз поменять форму.

Состояние	Пример	Насколько реально защитить
Исходный документ	Файл с расчётами, чертёж, клиентская база	Относительно легко
Конкретное решение	Формула цены, схема процесса, алгоритм отбора клиентов	Возможно, если оно точно описано и действительно охранялось
Настройка под компанию	Параметры модели, роли сотрудников, значения показателей	Зависит от доказательств и содержания договора
Обобщённый принцип	Понимание того, почему подобные компании теряют деньги	Значительно сложнее
Профессиональный навык	Умение быстро находить такую проблему у других клиентов	Почти невозможно монополизировать без фактического запрета на профессию

Это не юридическая классификация, а практическая карта местности. Она объясняет, почему спор о нарушении NDA часто оказывается спором не о фактах, а о том, как назвать случившееся. Компания говорит: «Он использовал нашу методику». Консультант отвечает: «Я применил собственный опыт».

Компания настаивает: «До работы с нами он этого не знал». Консультант разводит руками: «Именно поэтому вы меня и наняли, чтобы после совместной работы кто-нибудь начал понимать больше».

Самое интересное, что методика действительно может содержать одновременно и секрет клиента, и компетенцию консультанта. Клиент дал уникальные данные и живую среду, консультант принёс аналитический подход, соединил сведения, построил гипотезу и превратил всё это в работающую модель.

Назначать задним числом одного автора всему результату примерно так же продуктивно, как выяснять в семье, чей рецепт борща: того, кто купил продукты, или того, кто понял, что с ними делать.

Для договора отсюда следует практический вопрос: перешла ли готовая модель к заказчику и на каких правах. Подробно об этом в четвёртой части.

Парадокс консультационного бизнеса

У клиента обычно два вполне понятных желания. Он хочет, чтобы консультант принёс ему опыт, полученный в других компаниях, желательно большой, разнообразный и оплаченный другими. И хочет, чтобы всё знание, возникшее в его проекте, навсегда осталось внутри и больше никому не помогло.

По отдельности оба желания разумны. Вместе они складываются в изящную конструкцию: опыт должен свободно втекать в компанию и ни при каких обстоятельствах не вытекать обратно. Если бы это правило работало буквально, консультационный рынок бы исчез.

Каждый специалист после первого серьёзного проекта становился бы носителем юридически заражённого знания и до конца жизни работал бы только с первым клиентом. Для первого клиента новость хорошая, для экономики, конкуренции и самого понятия профессии заметно хуже.

Поэтому право разных стран и пытается провести границу между конкретным коммерческим секретом и общими знаниями, навыками и опытом человека. Проводят её по-разному, иногда жёстко, иногда в пользу мобильности работника или консультанта.

Вопрос при этом один: можно ли защищать конкурентное преимущество компании, не превращая защиту в право собственности на чужую память?

NDA не стирает память

Главная ошибка при подписании NDA состоит в ожидании технологического эффекта, которого договор дать не может. Он не удалит из головы консультанта увиденные закономерности и не отменит накопленный опыт.

Не заставит забыть, почему один проект провалился, а другой удался. И сам по себе не докажет, что похожее решение у другого клиента выросло именно из вашей конфиденциальной информации.

Работа у NDA скромнее, но полезная. Он обозначает, какие сведения стороны считают чувствительными, устанавливает правила обращения с документами и данными, запрещает очевидное раскрытие и может отдельно ограничить использование информации за пределами проекта.

Он даёт основание для требований, убытков, неустойки или судебного запрета. И превращает общее «я никому не расскажу» в более определённую договорённость.

Но между договорённостью и защитой лежит большая территория: секрет нужно определить, доступ ограничить, передачу зафиксировать, нарушение доказать, а связь между чужими действиями и своими потерями показать. В российской практике именно на этой территории многие грозные NDA становятся декоративными.

В папке с договорами они выглядят прекрасно, внушают уважение числом страниц и особенно убедительны в пункте о штрафе в десять миллионов рублей. А потом выясняется, что компания не может точно назвать конфиденциальную информацию, никаких правил обращения с ней не вводила, раздавала документы всем подряд и не знает, что именно ответчик раскрыл или использовал. Юридический бронепоезд оказывается картонной декорацией, причём очень хорошо согласованной юристами.

Значит ли это, что NDA бесполезен?

Нет. Ремень безопасности не предотвращает аварию, но выбрасывать его из-за этого никто не предлагает.

NDA сравнительно хорошо защищает от прямых и доказуемых действий: публикации внутренних документов, передачи клиентской базы, копирования чертежей, открытия доступа к закрытым материалам, пересылки коммерческих предложений конкуренту. Проще говоря, от нарушений, после которых остаются файлы, письма, сообщения и журналы доступа.

Гораздо хуже он защищает от тихого переноса понимания, когда человек ничего не копирует и никого не цитирует, но после проекта иначе думает, точнее спрашивает и быстрее находит решения.

Поэтому в России NDA работает не только как основание для иска, но и как институт доверия, усиленный возможностью наказать за особенно явное нарушение. Он сообщает сторонам, где проходит граница допустимого, с какими сведениями обращаться осторожно и что будет за сознательное предательство договорённостей.

Это немало. Бизнес держится не столько на готовности судиться, сколько на предсказуемости партнёров, и договор нужен не только чтобы выиграть суд, но и чтобы до суда не дойти.

Только доверие не стоит путать с магией. Подписанный NDA не создаёт вокруг информации силового поля. Чем абстрактнее предмет защиты, тем меньше результат зависит от суровости формулировок и тем больше от разумных границ, поведения сторон и качества доказательств.

Кому всё-таки принадлежит знание?

Предварительный ответ такой. За клиентом должны оставаться его данные, документы, конкретные закрытые решения и то конкурентное преимущество, которое он действительно создал и разумно охранял. За консультантом остаются его прежние методики, аналитический аппарат, общие профессиональные знания и опыт, сложившийся в работе, если, пользуясь ими, он не воспроизводит и не эксплуатирует конкретный секрет клиента.

Между этими территориями неизбежно останется серая зона, и чем интеллектуальнее работа, тем она шире. У токаря можно потребовать вернуть чертёж детали. У консультанта нельзя потребовать вернуть понимание того, почему ваша организационная структура не работает.

Поэтому задача хорошего NDA не в том, чтобы объявить секретом всё, что человек увидел, услышал, понял, предположил или когда-нибудь вспомнит. Такой договор выглядит грозно, но запрещает уже не нарушение, а мышление.

Разумный NDA проводит границу: вот чужой секрет, который нельзя раскрывать и использовать; вот результат совместного проекта, права на который определили заранее; а вот профессиональный багаж, который остаётся с человеком.

Эта граница существует не только в теории. Европейское, американское и британское право давно ищет баланс между охраной коммерческой тайны и свободой применять честно приобретённые навыки. Российское право тоже позволяет запрещать не только разглашение, но и использование конфиденциальной информации, однако российская судебная практика особенно наглядно показывает, как трудно перейти от грозного текста договора к доказанному нарушению. Сначала посмотрим, как с этим справляется мир, потом вернёмся в Россию.



ЧАСТЬ 2 ИЗ 6

Как мир делит секреты и человеческую память

Если после первой части кажется, что границу между чужим секретом и собственной компетенцией провести невозможно, мировой опыт предлагает утешение: провести её действительно невозможно, но суды и законодатели много лет всё равно пытаются.

Сначала о двух терминах, иначе дальше легко запутаться. NDA подписывают «на входе», когда человеку открывают информацию: чаще всего с консультантом или партнёром. С работниками в России обычно поступают иначе и знакомят их под подпись с перечнем сведений, составляющих коммерческую тайну.

Соглашение о неконкуренции, non-compete, работает «на выходе»: человек обещает какое-то время не работать у конкурентов. В России такое условие с работником почти не применяется, потому что ограничивает конституционное право на труд. Многие зарубежные дела ниже как раз о бывших работниках, и спор в них часто сводится к тому, не превращается ли NDA в non-compete.

Единого международного ответа нет, и разные страны порой приходят к противоположным выводам в почти одинаковых ситуациях. Один суд рассуждает так: человек знает планы прежнего работодателя настолько хорошо, что на новом месте будет ими пользоваться, даже если искренне пообещает этого не делать, поэтому его работу стоит на время ограничить.

Другой отвечает, что предположение о неизбежном использовании нельзя подменять доказательством, иначе любой NDA легко превратить в бессрочный запрет работать у конкурентов. Третий ищет середину: специалист продолжает работать, но не получает за счёт чужого секрета временную фору, тот самый «трамплин», который позволяет перепрыгнуть через месяцы исследований, проб и ошибок.

За этими различиями стоит один конфликт. Экономике одновременно нужно, чтобы компании могли сохранять созданные ими секреты и чтобы знания и люди могли перемещаться. Если защищать только компанию, рынок постепенно превратится в набор интеллектуальных княжеств с крепостными специалистами.

Если защищать только мобильность, вкладываться в уникальные разработки станет бессмысленно: первый же сотрудник или консультант, ушедший из проекта, разнесёт преимущество по всему рынку. Поэтому мировой опыт полезен не готовой формулой, а набором способов искать баланс.

Европейский союз: запретить можно использование секрета, но не профессию

Европейский подход довольно ясно отделяет разглашение от использования. В Директиве Европейского союза 2016/943 о защите коммерческой тайны статья 4 так и называется: «Неправомерное приобретение, использование и раскрытие коммерческой тайны». Приобретение описано в ней отдельно, а использование и раскрытие хотя и стоят рядом, но названы разными действиями.

Значит, человек может никому ничего не рассказать и всё равно нарушить права обладателя, если применит сведения вопреки договорной или иной обязанности ограничить их использование.

Например, консультант получил доступ к закрытой модели расчёта цен только для выполнения проекта. Если потом он применит эту модель у другого заказчика, проблема будет не в том, что он «разболтал» формулу, а в том, что использовал её за пределами цели, ради которой доступ давали.

Но не всякая полезная информация автоматически становится коммерческой тайной. В европейской конструкции она не должна быть общеизвестной или легкодоступной для тех, кто обычно работает с такими сведениями, должна иметь коммерческую ценность именно благодаря секретности и охраняться обладателем разумными мерами.

Последнее условие для владельца особенно неприятно. Право задаёт ему простой вопрос: если информация была такой ценной, почему вы обращались с ней как с меню в корпоративной столовой? Нельзя раздать документ всем сотрудникам, партнёрам и подрядчикам, не обозначив его статус и не ограничив доступ, а после появления похожего решения у конкурента вдруг обнаружить, что в файле лежала главная тайна европейского бизнеса.

При этом директива подчёркивает, что определение коммерческой тайны не охватывает малозначимую информацию, а также опыт и навыки, приобретённые работниками в обычном ходе работы, и не даёт оснований ограничивать использование работниками добросовестно приобретённых опыта и навыков.

Законными признаются и независимое создание решения, и изучение, разборка или тестирование продукта, который общедоступен или законно находится у изучающего, если тот не связан обязанностью, например договорной, этого не делать.

Автоматического иммунитета консультантам это не даёт, но принцип виден: право охраняет определённый секрет, а не весь интеллектуальный результат человеческой деятельности. [Директива ЕС 2016/943, статьи 1–4, вводные положения 14 и 16](#)

Для нашего разговора европейская логика сводится к двум утверждениям, которые действуют одновременно:

Нельзя использовать конкретный чужой секрет только потому, что удалось его запомнить.

Нельзя объявить чужим секретом всё, чему человек научился во время работы.

Между этими фразами и помещается почти весь будущий спор.

США: когда секрет неизбежно «просачивается» в решения

Американский федеральный закон тоже считает использование коммерческой тайны самостоятельной формой нарушения. По *Defend Trade Secrets Act* неправомерное присвоение может выражаться не только в раскрытии, но и в использовании секрета лицом, которое знало или должно было знать, что сведения получены при обстоятельствах, обязывающих хранить их в тайне или ограничивать их применение.

Как и в Европе, обладатель должен показать, что информация была ценна, потому что оставалась неизвестной и не могла быть легко установлена законными способами, и что он принимал разумные меры для сохранения секретности. [18 U.S.C. § 1839](#)

При этом «американская практика» не единая кнопка. Федеральный закон появился только в 2016 году, а до него и параллельно с ним действуют законы штатов, и к доктрине, о которой пойдёт речь дальше, суды штатов относятся по-разному.

Интереснее другое: спор вокруг доктрины **inevitable disclosure**, «неизбежного раскрытия», а для нашей темы точнее сказать, неизбежного использования. Её логика в том, что иногда новая должность человека так тесно связана с его знаниями о прежней компании, что отделить профессиональные решения от чужих секретов практически невозможно.

Классическим примером стало дело **PepsiCo v. Redmond**, которое решалось по закону штата Иллинойс: федерального закона тогда ещё не было. Уильям Редмонд руководил крупным подразделением PepsiCo и знал её планы, цены и маркетинговые бюджеты. В конце 1994 года он перешёл к прямому конкуренту, в Quaker Oats, владевшую Gatorade.

PepsiCo не утверждала, что Редмонд уже передал конкуренту какой-то документ. Её довод был другим: на новой работе он просто не сможет не учитывать известные ему планы.

Суд согласился, что риск не сводится к сознательной передаче файлов. Даже добросовестный человек, принимая решения для нового работодателя, будет опираться на то, что знает о будущих шагах конкурента. Апелляционный суд сравнил PepsiCo с тренером, чей игрок накануне важного матча ушёл к сопернику, прихватив книгу розыгрышей.

В итоге суд поддержал запрет, наложенный первой инстанцией: Редмонду не разрешили приступать к новой работе до мая 1995 года, то есть примерно полгода, и бессрочно запретили использовать и раскрывать секреты PepsiCo. [PepsiCo, Inc. v. Redmond, 54 F.3d 1262 \(7th Cir. 1995\)](#)

Подход выглядит убедительно. Если новый директор по продажам знает, в каком регионе конкурент через два месяца снизит цены и сколько вложит в продвижение, просить его «просто не учитывать» эти сведения довольно наивно. Примерно как просить шахматиста забыть подготовленную соперником комбинацию, которую он успел разглядеть.

Но в таком рассуждении спрятана опасность. Если достаточно одного предположения о неизбежном использовании, доказывать само нарушение уже не нужно, и компания может ограничивать будущую работу человека, хотя тот подписывал только соглашение о конфиденциальности, а не о неконкуренции.

NDA незаметно превращается из договора о сохранении тайны в договор о том, где человеку разрешено работать.

Калифорния: подозрение ещё не доказательство

Против такой подмены выступили суды Калифорнии, где профессиональную мобильность защищают традиционно: соглашения, ограничивающие человека в занятии профессией, там по общему правилу ничтожны. [Cal. Bus. & Prof. Code § 16600](#)

В деле **Whyte v. Schlage Lock** (2002) вице-президент Schlage по продажам Дуглас Уайт, отвечавший в том числе за работу с The Home Depot, перешёл на аналогичную должность в прямого конкурента, компанию Kwikset. Соглашение о конфиденциальности он подписывал, о неконкуренции нет.

Калифорнийский апелляционный суд прямо отверг доктрину неизбежного раскрытия: нельзя запретить бывшему сотруднику работать у конкурента только потому, что новые обязанности предположительно заставят его пользоваться известными ему секретами. Такая конструкция задним числом создаёт соглашение о неконкуренции, которого стороны не подписывали.

Для вмешательства нужны доказательства фактического незаконного использования или достаточно конкретной угрозы, а не общий довод «он слишком много знает и наверняка что-нибудь применит». Показательно, что часть сведений Уайта суд признал коммерческой тайной и всё равно отказал в запрете, потому что доказательств реального или угрожающего незаконного использования Schlage не представила. [Whyte v. Schlage Lock Co., 101 Cal. App. 4th 1443 \(2002\)](#)

Так в американском праве сложились два полюса. В логике PepsiCo новая роль может сделать использование секрета практически неизбежным, и тогда есть риск, что NDA превратится в скрытый запрет конкуренции.

В логике Whyte без доказанного использования работу человека ограничивать нельзя, и тогда есть риск, что компания не успеет защититься, пока секрет не применили.

Федеральный DTSA, появившийся позже, ближе к калифорнийской логике. Он прямо запрещает судебным запретом не допускать человека до новой работы, а ограничения должны опираться на доказательства угрозы незаконного использования, а не просто на то, что человек

что-то знает. [18 U.S.C. § 1836\(b\)\(3\)\(A\)](#)

Так что ссылка на Америку без уточнения юрисдикции примерно так же содержательна, как ссылка на «зарубежный опыт управления»: звучит солидно, а решать всё равно придётся самим.

Для российского бизнеса важен не выбор между PepsiCo и Калифорнией, а сам вопрос. Достаточно ли того, что человек имел доступ к информации и теперь работает с конкурентом, или нужно показать, **какой именно секрет он использовал и в каком решении это проявилось?** Российский суд, как будет видно дальше, обычно хочет второго.

Великобритания: не всякая конфиденциальная информация переживает увольнение

Британская практика дала ещё одну полезную конструкцию: служебную информацию делят по степени защищённости. Обычно её связывают с делом **Faccenda Chicken Ltd v. Fowler**.

Компания торговала свежими цыплятами с развозных фургонов-рефрижераторов. Её менеджер по продажам Барри Фаулер уволился и открыл конкурирующую фирму в том же районе, вслед за ним ушли восемь сотрудников.

Работодатель утверждал, что они пользуются известными им сведениями о продажах: адресами клиентов, маршрутами, обычными заказами, днями и временем доставки, индивидуальными ценами.

Условий о конфиденциальности в трудовых договорах не было вовсе, поэтому суду пришлось решать, какая информация охраняется после увольнения сама по себе, без всякого специального запрета.

Классификацию сформулировал судья первой инстанции, а Апелляционный суд Англии в 1985 году её уточнил. Работодатель проиграл: сведения о продажах суд коммерческой тайной не признал. [Faccenda Chicken Ltd v Fowler \[1987\] Ch 117, текст решения](#)

Упрощённо британская логика различает три уровня. Общеизвестные или малозначимые сведения человек использует свободно. Конфиденциальными сведениями нельзя злоупотреблять, пока работаешь, но после увольнения подразумеваемый запрет на них уже не распространяется. А настоящие коммерческие секреты настолько конфиденциальны, что обязанность не использовать и не раскрывать их может пережить сами трудовые отношения.

По мнению апелляционного суда, после увольнения охраняются только коммерческие тайны и сведения, равноценные им по степени секретности. Чтобы понять, к какому уровню относится информация, суд смотрит на характер работы сотрудника, на сами сведения и круг допущенных к ним людей, на то, давал ли работодатель понять, что сведения конфиденциальны, и можно ли отделить их от обычных профессиональных знаний.

Смысл не в том, что всё запомненное автоматически становится свободным: намеренно заучить или скопировать список клиентов, пока работаешь, по-прежнему нарушение. И не в том, что бумага всегда защищена, а память всегда свободна.

Любопытно, что в самом деле Faccenda довод о памяти сработал против работодателя: продавцы и так быстро запоминали всё о своём районе, и суд увидел в этом признак обычного рабочего знания, а не тайны.

Главное в другом: после окончания отношений нельзя одинаково обращаться с подлинной технологической тайной и со знанием того, какие покупатели обычно заказывают по четвергам.

Так британская традиция спрашивает владельца информации не только о секретности, но и о качестве самого секрета. Насколько он специфичен и можно ли его точно определить? Чем он отличается от отраслевого опыта?

Может ли специалист продолжать работать, не пользуясь им? Если на последний вопрос ответить нельзя, запрет использования начинает подозрительно напоминать запрет профессии.

«Трамплин»: знания не отнять, а нечестную фору можно

Ещё один британский инструмент называется **springboard doctrine**, доктрина трамплина. Её идея в том, что конфиденциальная информация, использованная с нарушением, может дать конкуренту временное преимущество, даже если позже сама информация перестанет быть секретной.

Истоки доктрины в решении судьи Роксбурга по делу Terrapin v Builders Supply 1959 года: тот, кто получил сведения по секрету, не вправе использовать их как трамплин во вред доверившему, и трамплином они остаются, даже когда все детали уже опубликованы. [Terrapin Ltd v Builders Supply Co \(Hayes\) Ltd, \[1967\] RPC 375](#)

Представим, что компания два года разрабатывала технологический процесс. Конкурент получил её материалы и воспроизвёл результат за два месяца, а ещё через какое-то время ключевые элементы технологии стали публичными.

Можно рассуждать так: раз информация теперь доступна всем, запрещать её бессмысленно. Но конкурент уже получил то, чего не было у остальных, и перепрыгнул через два года исследований, затрат и неудачных опытов.

В такой ситуации суд может ограничить использование результата на срок, нужный, чтобы отнять незаконно полученную фору. Позднейшая практика подчёркивает, что преимущество трамплина не вечно, а сам запрет защищает пострадавшего, но не наказывает нарушителя, поэтому он не должен быть шире и дольше необходимого (Roger Bullivant v Ellis, 1987; Forse v Secarma, 2019).

Цель в том, чтобы не стирать знания из головы нарушителя и не дарить первой компании вечную монополию, а вернуть стороны примерно туда, где они были бы без нарушения. [Обзор практики springboard injunctions, Gaby Hardwicke](#)

Взгляд довольно зрелый. Время назад не повернуть, память судебным решением не очистить, а ставшее публичным знание снова секретным не сделать. Зато можно не дать человеку превратить нарушение в бесплатное ускорение.

Для консультационной практики из этого следует, что спорить иногда стоит не о бессрочном «никогда больше так не делай», а о конкретном преимуществе, полученном благодаря доступу к чужому решению.

Residual knowledge: право пользоваться тем, что осталось в памяти

Американская договорная практика, прежде всего в сделках M&A и соглашениях об интеллектуальной собственности, выработала ещё один ответ: **residuals clauses**, оговорки об остаточных знаниях. Такая оговорка разрешает получателю использовать сведения, которые сохранились в обычной памяти его сотрудников без опоры на документы.

Логику получателя понять можно. Крупная консультационная, технологическая или инвестиционная компания каждый день видит сотни решений и не может гарантировать, что сотрудники забудут все идеи после переговоров. К тому же потом почти невозможно установить, из какого проекта человек впервые вынес общее понимание проблемы.

Для раскрывающей стороны такая оговорка опасна. Если разрешить использовать всё, что человек «просто запомнил», NDA рискует стать соглашением о законном присвоении информации при условии хорошей памяти и предусмотрительно закрытого ноутбука. Поэтому residuals clause не общепризнанное право консультанта и не норма закона, а результат переговоров.

Раскрывающая сторона обычно добивается ограничений: оговорка действует только без намеренного запоминания и обращения к записям, не даёт лицензии на патенты, авторские права и другие объекты интеллектуальной собственности, не разрешает раскрывать информацию и не распространяется на коммерческую тайну и особо чувствительные сведения.

Иногда отдельно запрещают использовать остаточные знания для разработки конкурирующей технологии. [Residual Clauses in an NDA for M&A Transactions, Venable](#), [Residuals Clauses in IP Agreements and NDAs, Morgan Lewis](#)

По сути, стороны заранее признают очевидное: человеческая память существует. А потом договариваются, каких последствий из этого быть не должно.

Что из мирового опыта следует для консультанта и клиента

При всех различиях европейский, американский и британский подходы сходятся в нескольких точках.

Неразглашение и неиспользование считаются разными обязанностями. Если клиент хочет ограничить именно применение информации, это нужно формулировать отдельно, потому что запрет «не рассказывать третьим лицам» сам по себе не отвечает на вопрос, вправе ли консультант пользоваться полученным знанием в своей работе.

Защищается не всё полезное, а определённый секрет. Компания должна уметь его назвать и объяснить, почему он не был общеизвестен, чем был ценен и как охранялся.

Похожий результат ещё не доказывает использования. Два консультанта вполне могут прийти к одному выводу независимо, особенно если речь не о химической формуле, а о довольно земной рекомендации считать маржинальность по каналам продаж.

Да и доступ к секрету не всегда означает его применение: подозрение может быть разумным, но право обычно хочет видеть действия, решения, документы, совпадения, переписку, экономическую выгоду или хотя бы конкретную угрозу.

Слишком широкий NDA начинает работать как non-compete. Если человеку запрещено применять любое знание из проекта, работать с любыми компаниями отрасли и использовать любые похожие методы, предметом договора становится уже не конфиденциальность, а его будущая профессиональная жизнь.

Наконец, у нарушения может быть временной эффект. Чужой секрет способен не только дать готовый результат, но и сократить путь к нему, поэтому разумная защита иногда должна отбирать незаконную фору, а не пытаться навсегда остановить движение знаний.

Мир не нашёл идеальной границы, и это тоже результат

Мировой опыт не даёт клиенту универсального права сказать: «Всё, чему вы у нас научились, теперь наше». Но и консультанту он не позволяет прикрыть словом «опыт» копирование конкретной модели, технологии или стратегии.

Перенести файл и перенести компетенцию не одно и то же, однако между ними много промежуточных состояний: запомненная формула, воспроизведённая логика, чуть изменённая методика, подсказанное решение, сокращённый путь.

Главный принцип можно сформулировать так:

Компания вправе защищать созданный ею секрет и полученное за его счёт конкурентное преимущество, но не вправе приватизировать всю профессиональную эволюцию человека, которому этот секрет стал известен.

А консультант вправе становиться опытнее после каждого проекта, только слово «опыт» не индульгенция на перенос чужих разработок.

В теории всё звучит почти примиряюще. На практике спор возвращается к скучным и решающим деталям: что именно передали и зачем, как это охранялось, что запретил договор, какое решение появилось у конкурента и можно ли доказать причинную связь.

В России закон тоже умеет запрещать использование конфиденциальной информации, но на практике суд больше доверяет вещественному. Ему гораздо удобнее разбираться с похищенным чертежом, пересланной базой или опубликованным документом, чем с утверждением:

— Уважаемый суд, он ничего не украл. Он просто слишком хорошо нас понял.



ЧАСТЬ 3 ИЗ 6

Российский NDA: три этажа защиты и одна лестница доказательств

После европейских директив, американских доктрин и британских «трамплинов» легко заподозрить, что российское право просто не добралось до вопроса об использовании чужих знаний. Это не так. Запретить использование конфиденциальной информации в России можно, как можно потребовать прекратить нарушение, вернуть документы, возместить убытки и взыскать договорную неустойку. При определённых обстоятельствах информацию защищают и как секрет производства, ноу-хау.

Российское право здесь похоже на хорошо укомплектованный гараж: все инструменты на месте, но перед ремонтом владелец не помнит, куда положил ключи, не составил список деталей и не может толком показать, какая машина вообще его.

Поэтому главный российский вопрос не в том, можно ли запретить использование конфиденциальной информации. Можно. Главный вопрос в другом: сможет ли компания доказать, что у неё был определённый секрет, что она передала его конкретному человеку на ограниченных условиях и что потом использовали именно этот секрет?

Чем ближе спор к документу, чертежу или клиентской базе, тем увереннее чувствует себя суд. Чем ближе он к знаниям, выводам и опыту консультанта, тем быстрее юридическая определённость растворяется в тумане.

Три способа защищать информацию

Под словом NDA в российской практике часто скрываются три разных правовых механизма. Пользоваться ими можно одновременно, но требования и последствия у них разные.

Механизм	Что защищает	На чём основано требование
Договорная конфиденциальность	Сведения, которые стороны договорились не раскрывать или не использовать	На нарушении конкретного обязательства
Режим коммерческой тайны	Информацию, в отношении которой введён предусмотренный законом режим	На нарушении правил обращения с коммерческой тайной
Ноу-хау	Ценные секретные сведения о способах профессиональной деятельности, технологиях, процессах и решениях	На нарушении исключительного права

Механизмы пересекаются, но синонимами не становятся. Компания может заключить NDA, не вводя полноценного режима коммерческой тайны, и тогда защищает прежде всего договорное обязательство контрагента. Может ввести режим и подробно урегулировать доступ сотрудников и подрядчиков.

А может признать конкретную технологию или методику секретом производства и защищать уже не только договор, но и исключительное право на ноу-хау.

Ошибка начинается, когда компания выбирает самое торжественное название, скажем «Соглашение о защите коммерческой тайны и ноу-хау», а внутри оставляет единственную содержательную фразу: «Всё, что стало известно сторонам, является конфиденциальным». Юридическая ценность документа от высоты заголовка не зависит.

Для сведений под режимом коммерческой тайны есть ещё и публично-правовая защита. Незаконно разгласить или использовать коммерческую тайну без согласия владельца, если она была доверена или стала известна по службе или работе, уже преступление, даже без всякого ущерба.

Крупный ущерб или корыстный мотив ужесточают наказание вплоть до лишения свободы на срок до пяти лет. [Статья 183 УК РФ](#) Если до уголовного дела не дошло, возможен административный штраф. [Статья 13.14 КоАП РФ](#) Обе статьи защищают тайну, охраняемую законом, поэтому сведения, закрытые только договором, под них не попадают.

Первый этаж: договорный запрет

Гражданский кодекс закрепляет свободу договора: стороны сами определяют свои обязанности, если те не противоречат закону. Поэтому заказчик и консультант вправе договориться не только о неразглашении информации, но и об ограничении её использования. [Статья 421 ГК РФ](#)

Показательно, как устроена норма, которая действует и без всякого NDA. Сторона договора подряда, получившая информацию о новых решениях и технических знаниях, в том числе не защищаемых законом, а также сведения, в отношении которых установлен режим коммерческой тайны, не вправе сообщать их третьим лицам без согласия другой стороны, а порядок и условия пользования такой информацией закон оставляет на усмотрение сторон. [Статья 727 ГК РФ](#)

Обратите внимание на слова «в том числе не защищаемых законом»: для этой части нормы режим коммерческой тайны не нужен, достаточно того, что сведения получены при исполнении договора.

Эти правила распространяются и на возмездное оказание услуг, то есть на консалтинг. [Статья 783 ГК РФ](#) Выходит, что запрет разглашения закон подразумевает сам, а запрет использования нужно прописать.

Особой ответственности для внешнего исполнителя Закон о коммерческой тайне не устанавливает, [статья 14 Закона о коммерческой тайне](#) поэтому всё, что компания хочет взыскать с консультанта, должно быть записано в договоре.

Можно, например, записать, что переданная информация используется только для конкретного проекта, не применяется в интересах самого консультанта или третьих лиц, не используется при работе с перечисленными конкурентами в течение согласованного срока, не воспроизводится полностью или в существенной части в других методиках и продуктах и возвращается или уничтожается после завершения работ.

Однако фраза «запрещается использовать конфиденциальную информацию» решает только половину задачи. Вторая половина состоит в том, чтобы определить, что считается использованием: применение конкретной модели расчёта, изготовление продукта по переданному чертежу, коммерческое предложение с полученными ценами, звонки клиентам из закрытой базы, воссоздание технологического процесса, обучение чужих сотрудников по материалам заказчика.

Если этого не сделать, спор уйдёт в толкование. Заказчик будет говорить: «Он использовал наши знания». Консультант ответит: «Я использовал свой мозг». И суду придётся выяснять содержание договора уже после конфликта, в самый дорогой для этого момент.

Дело о коммерческом предложении: договор может приравнять использование к разглашению

Хороший пример договорного подхода даёт дело № А45-47738/2018. Новосибирская компания «Функе Сибирь» привлекала клиентов через агента-предпринимателя. В компанию пришёл запрос потенциального клиента на теплообменники, и агент о нём знал, потому что сам переслал письмо руководству.

А затем со своей почты отправил этому клиенту коммерческое предложение конкурирующей организации. Клиент письменно подтвердил, что предложения от «Функе Сибирь» так и не получил.

В договоре на такой случай была важная формулировка: под разглашением конфиденциальной информации понимается также её использование в личных целях. Договор заранее расширил обычное значение слова «разглашение» и включил в него применение сведений в собственных интересах.

Компания потребовала предусмотренный договором штраф в 200 000 рублей. Суд первой инстанции признал разглашение, но снизил штраф до 100 000 рублей, потому что нарушение было единичным, а убытков истец не показал.

Апелляция решение оставила в силе. [Решение Арбитражного суда Новосибирской области по делу № А45-47738/2018, постановление Седьмого арбитражного апелляционного суда от 17.06.2019](#)

Для нашей темы пример показателен тем, что ответчик ничего не вывешивал на сайте и не рассылал неопределённому кругу лиц. Он воспользовался полученной возможностью и информацией, чтобы увести сделку.

Сработала не абстрактная конфиденциальность, а конкретная конструкция: деловые отношения, информация, полученная в их рамках, договор, который охватывал использование в личных целях, материальное доказательство в виде чужого коммерческого предложения и заранее определённый штраф. Между секретом и выгодой ответчика получилась короткая доказательственная цепочка.

Второй этаж: режим коммерческой тайны

Если компания хочет ссылаться именно на режим коммерческой тайны, одного NDA мало. Статья 10 Федерального закона № 98-ФЗ требует от обладателя информации целого комплекса мер:

1. определить перечень сведений, составляющих коммерческую тайну;
2. ограничить доступ: установить порядок обращения с информацией и контролировать его соблюдение;
3. учитывать лиц, получивших доступ или которым информация была передана;
4. урегулировать использование информации работниками через трудовые договоры, а контрагентами через гражданско-правовые;
5. наносить на материальные носители или включать в документы гриф «Коммерческая тайна» с указанием обладателя (для организации полное наименование и место нахождения).

Режим считается установленным только после принятия этих мер. [Статья 10 Закона о коммерческой тайне](#)

Этот момент бизнес особенно не любит. Собственнику кажется, что секрет существует, раз сам он считает информацию секретной. Закон на это отвечает, что внутренние переживания имеют большое человеческое значение, но для правовой охраны хотелось бы увидеть перечень, порядок доступа, учёт получателей и маркировку документов.

Здесь и проявляется главное противоречие российской практики. Компании хотят определить секрет как можно шире, а охранять его как можно менее обременительно. Суд требует обратного: чем шире заявлена тайна, тем труднее доказать, что с каждым её элементом действительно обращались как с тайной.

Если «конфиденциальным» объявлено всё, от стратегии развития до графика уборки офиса, возникает законный вопрос, понимали ли сами сотрудники разницу между секретом и обычной рабочей информацией.

Третий этаж: ноу-хау

Для консультантов самый интересный механизм связан с правом на секрет производства. Статья 1465 ГК РФ позволяет признать ноу-хау сведения любого характера (производственные, технические, экономические, организационные и другие) о результатах интеллектуальной деятельности в научно-технической сфере и о способах осуществления профессиональной деятельности.

Для этого сведения должны иметь действительную или потенциальную коммерческую ценность из-за неизвестности третьим лицам, не находиться в свободном законном доступе и охраняться обладателем разумными мерами. Режим коммерческой тайны назван одним из возможных способов такой охраны, но смысл нормы шире: обладатель должен показать реальные и разумные действия по сохранению конфиденциальности. [Статья 1465 ГК РФ](#)

Исключительное право на ноу-хау позволяет использовать его по своему усмотрению и запрещать использование другим, причём отсутствие запрета не считается разрешением. [Статья 1466 ГК РФ](#), [статья 1229 ГК РФ](#)

Нарушение, следовательно, возможно и без публичного раскрытия: закон прямо называет нарушителем того, кто неправомерно получил сведения и «разгласил или использовал» их. [Статья 1472 ГК РФ](#)

У той же нормы есть оборотная сторона, очень важная для консультантов. Тот, кто добросовестно и независимо от других пришёл к тем же сведениям, получает собственное, самостоятельное исключительное право на этот секрет производства (пункт 2 статьи 1466 ГК РФ). Совпадение результата само по себе нарушителем ещё не делает.

Если подрядчик получил технологию производства детали, никому её не сообщил, но начал выпускать такую же продукцию сам, это может оказаться незаконным использованием ноу-хау. Если консультант получил уникальную модель оптимизации ассортимента и воспроизвёл её у конкурента, теоретически возникает тот же вопрос.

Только слово «теоретически» здесь выполняет тяжёлую юридическую работу. Компании придётся показать, что перед судом не здравый управленческий совет, не общеизвестный отраслевой подход и не сумма опыта специалиста, а определённая, секретная и коммерчески ценная система знаний.

Назвать ноу-хау «методикой повышения эффективности бизнеса» мало, иначе исключительное право распространилось бы на заметную часть деловой литературы и примерно на половину выступлений бизнес-консультантов после второго бокала на конференции.

Дело о 299 чертежах: как выглядит работающая доказательственная цепочка

Одно из самых наглядных дел об использовании конфиденциальной информации рассматривалось под № А53-380/2021. Заказчик, ООО «Интермашхолдинг», передал подрядчику, азовскому ООО «Югточмаш», пакет конструкторской документации для изготовления трёхплунжерных насосов.

Одновременно с договором подряда стороны заключили отдельное соглашение о конфиденциальности: сведения предоставляются только для выполнения конкретных работ и в других целях без дополнительного согласования не используются.

Передачу оформили актом, где перечислялся пакет документации из 299 наименований, а сами материалы были прямо отнесены к коммерческой тайне и конфиденциальной информации. Заказчик дважды письменно требовал вернуть документацию, подрядчик требования не исполнил.

Зато нотариус зафиксировал на сайте подрядчика и на отраслевой торговой площадке предложения о поставке таких же насосов вместе с фотографиями.

Заказчик потребовал вернуть материалы и взыскать договорный штраф в три миллиона рублей. Документацию подрядчик вернул уже в ходе процесса, и от этого требования истец отказался. Главным стало другое: суды установили, что подрядчик использовал полученные сведения в своей коммерческой деятельности.

Штраф снизили до одного миллиона рублей, апелляция и кассация решение оставили в силе, а Верховный суд отказал в передаче жалобы на пересмотр. [Постановление Пятнадцатого арбитражного апелляционного суда от 02.09.2021, постановление Арбитражного суда Северо-Кавказского округа от 23.11.2021 № Ф08-11986/21, определение Верховного суда от 04.03.2022 № 308-ЭС22-1504](#)

Защита сработала не потому, что NDA набрали особенно грозным шрифтом. У заказчика была последовательность доказательств: конкретная документация и точный перечень из 299 позиций, акт передачи, определённая цель и прямой запрет на иные цели, обязанность вернуть носители и письменные требования о возврате, наконец, нотариально зафиксированные действия получателя на рынке.

Это почти идеальная противоположность ситуации, когда консультанту два года пересылают файлы в мессенджере, а после ссоры объявляют всю переписку сверхсекретной.

Дело о публичном доступе: суд хорошо видит открытую дверь

В деле № А56-92673/2016 петербургская компания «ВИАКАРД», процессинговый оператор топливных карт, дала партнёру, ООО «Терминал Сервис», доступ к своей системе через защищённый личный кабинет и подписала с ним соглашение о неразглашении.

Партнёр разместил на своём сайте кнопку «Поработайте с личным кабинетом в демо-режиме»: создал демонстрационную учётную запись и открыл доступ без пароля неопределённому кругу лиц.

Экспертиза насчитала 633 записи об авторизации. Апелляционный суд признал открытие кабинета без логина и пароля разглашением конфиденциальной информации и взыскал предусмотренный NDA штраф в 400 000 рублей. Этим спор не ограничился: вместе с компенсацией за нарушение прав на программу и договорным штрафом за реверс-инжиниринг (разбор программы ради воспроизведения её устройства) общая сумма взыскания превысила 40 миллионов рублей.

Суд по интеллектуальным правам решение оставил в силе, Верховный суд отказал в пересмотре. [Постановление Тринадцатого арбитражного апелляционного суда от 11.07.2018, постановление Суда по интеллектуальным правам от 31.10.2018 № С01-843/2018](#)

Пример важен не столько размером взыскания, сколько удобством доказательства. Был защищённый ресурс и учётная запись, был открытый доступ без пароля, были журналы авторизации и экспертиза, которая их прочитала. С такими обстоятельствами российский суд работать умеет: нарушение оставило цифровые следы и описывается обычными глаголами «создал», «открыл», «предоставил», «вошёл».

Совсем иначе звучит жалоба «после работы с нами консультант стал задавать конкуренту подозрительно правильные вопросы».

«Кронвет»: секрет, который не оформили как секрет

Обратный пример даёт дело № А56-53278/2017. Компания «Кронвет» пыталась запретить научному институту птицеводства, ФНЦ «ВНИТИП» РАН, использовать технологию производства вакцины против инфекционного бронхита кур и взыскать упущенную выгоду. На уровне здравого смысла объект выглядел идеальным кандидатом в ноу-хау: технология производства вакцины явно может стоить денег.

Но три инстанции отказали. Гриф «Коммерческая тайна» стоял только на служебном задании на разработку технологии, а технологического регламента изготовления вакцины, того самого документа, где и содержался секрет, с таким грифом в деле не оказалось. Режим коммерческой тайны суды сочли неустановленным.

Был и второй, самостоятельный мотив: технологию создавали специалисты, работавшие одновременно у истца и у ответчика, и суды пришли к выводу, что институт пользовался сведениями с ведома и согласия самой компании. [Постановление Суда по интеллектуальным правам от 11.10.2018 № С01-808/2018 по делу № А56-53278/2017](#)

Вывод неприятный, но полезный: ценность технологии сама по себе не доказывает, что охраняемое ноу-хау существует. Можно создать действительно уникальное решение и проиграть спор, если нельзя показать, что секрет определили, зафиксировали и защитили и что сама компания не пустила к нему людей, работавших одновременно на неё и на ответчика.

Неоформленный секрет похож на незапатентованное убеждение собственника в своей гениальности: возможно, оно совершенно справедливо, но суду нужно что-то более материальное.

Дело о стоматологических штифтах: чужая выручка ещё не ваши убытки

В деле № А82-14097/2022 угличское ООО «Форма», производитель стоматологических штифтов, требовало солидарно взыскать 47,4 миллиона рублей упущенной выгоды с конкурента и со своего же участника, владевшего половиной долей. По версии истца, участник учредил конкурирующую компанию и передавал ей коммерческую информацию о деятельности «Формы».

Три инстанции отказали. Истец не доказал ни полного комплекса мер по защите конфиденциальности, ни самого наличия секрета производства. Расчёт убытков, построенный на доходах конкурента, суды отклонили: он не учитывал других факторов, влияющих на доход, и не подтверждал причинную связь между предполагаемой передачей секрета и потерями истца.

Часть требований отпала ещё и из-за пропуска исковой давности. [Постановление Арбитражного суда Волго-Вятского округа от 26.12.2023 № Ф01-7749/2023, обзор практики защиты ноу-хау, Право.ру](#)

Это вторая большая ловушка после доказывания самого нарушения. Допустим, компания доказала, что её информацию использовали; теперь нужно показать размер потерь. Но выручка конкурента не равна убыткам истца. Конкурент мог продавать благодаря своей клиентской базе, бренду, оборудованию, людям и вложениям, и даже если чужое знание помогло ему выйти на рынок быстрее, придётся установить, какую часть результата дало именно оно.

В договорном споре эту проблему отчасти снимает неустойка: требуя её, кредитор не обязан доказывать убытки, и выводить стоимость секрета из движения звёзд и квартальной выручки ответчика не приходится. [Статья 330 ГК РФ](#) Однако явно несоразмерную неустойку суд может снизить. [Статья 333 ГК РФ](#)

Поэтому пункт «штраф 100 миллионов рублей за каждый случай» прекрасно дисциплинирует переговоры, но не гарантирует появления 100 миллионов на счёте истца.

Для ноу-хау это особенно важно. В отличие от авторских прав, закон не даёт обладателю секрета производства права требовать компенсацию вместо убытков, только доказанные убытки. [Статья 1472 ГК РФ](#)

В деле «ВИАКАРД» компенсацию взыскали за нарушение прав на программу, а не за секрет. Так что для секретов договорная неустойка едва ли не единственный способ не доказывать размер потерь.

LEVITA: большой штраф возможен, но новая эпоха ещё не наступила

В 2026 году заметным стало дело № А40-14982/2025, связанное с сетью студий растяжки и балета LEVITA. Бывший франчайзи вёл Telegram-канал, где, по словам представителя франчайзера, системно публиковал сведения о внутренней деятельности сети.

Договор концессии предусматривал за разглашение конфиденциальной информации штраф в 30 миллионов рублей, и франчайзер сам снизил требование вдвое.

Решением от 3 марта 2026 года Арбитражный суд Москвы взыскал штраф за разглашение в 15 миллионов рублей, а вместе с роялти, пени и другими штрафами общая сумма достигла примерно 17,5 миллиона рублей.

Ответчик заявил, что будет обжаловать решение. [Forbes: суд оштрафовал франчайзи на 15 млн рублей за разглашение конфиденциальной информации](#)

Сумма впечатляет, особенно на фоне привычного снижения договорных штрафов. Представители франчайзера называют её рекордом для таких споров, а опрошенные Forbes юристы отмечают, что прежде за разглашение взыскивали максимум около миллиона рублей. Но объявлять по одному свежему решению революцию в российской практике рано.

Речь опять шла о публикациях в канале, то есть о материально зафиксированном раскрытии сведений, а не о применении усвоенного знания. Исход конкретного дела зависит от текста договора, поведения ответчика, содержания опубликованных материалов и процессуальной позиции сторон.

И связанные споры кончаются по-разному: по параллельному иску того же франчайзера к тому же бывшему партнёру суд сначала присудил лишь небольшой штраф, а кассация отменила решение и отправила дело на новое рассмотрение. Одинаково суровый договор не избавляет от необходимости доказывать каждое конкретное нарушение.

Крупный штраф подтверждает, что у NDA бывают зубы. Пока, правда, это зубы для достаточно заметной добычи.

Даже подпись сторон не создаёт ноу-хау автоматически

Ещё один важный поворот появился в практике Верховного суда в 2025 году. В деле № А65-31236/2023 предприниматели заключили лицензионный договор на использование ноу-хау, инструкций по открытию стриминговой студии: паушальный взнос 1,59 миллиона рублей плюс роялти.

Лицензиат заплатил больше миллиона, решил, что получил общедоступные сведения, и потребовал признать договор незаключённым и вернуть деньги. Три инстанции отказали: предмет договора согласован, договор исполнялся, материалы приняты по акту без замечаний.

В июле 2025 года Верховный суд эти акты отменил. Суды должны были выяснить, что конкретно было предметом договора и являются ли переданные сведения секретом производства, то есть есть ли у них коммерческая ценность, нет ли к ним свободного доступа и принимались ли разумные меры конфиденциальности.

Название договора и подписанный акт приёма-передачи этого не заменяют. Более того, Верховный суд указал, что при отсутствии ноу-хау отношения сторон нужно квалифицировать иначе, например как оказание консультационных услуг. Дело направлено на новое рассмотрение. [Определение Судебной коллегии по экономическим спорам Верховного суда от 25.07.2025 № 306-ЭС25-461, разбор дела, «Коммерсантъ»](#)

Для консультантов это принципиально. Если стороны напишут, что «все идеи, знания, навыки и методы, обсуждавшиеся в ходе проекта, являются ноу-хау заказчика», суд не обязан принимать эту формулу за объективную реальность.

Договор создаёт обязательство, но не способен превратить общеизвестный SWOT-анализ, систему еженедельных совещаний или формулу валовой маржи в уникальный результат интеллектуальной деятельности.

Ярлык «ноу-хау» в договоре суд проверит так же, как проверил бы сведения и без всякого договора.

Почему российскому суду трудно поймать умного консультанта

Вернёмся к исходной ситуации. Консультант не передавал документов, не раскрывал названия клиента, не копировал методику буквально и не звонил людям из клиентской базы. Он увидел закономерность, соединил её с прежним опытом и применил новое понимание в следующем проекте.

Что должен доказать первый клиент, зависит от того, на что он опирается. Если на договор, например требует неустойку по NDA, ему нужно показать:

1. Договор запрещал не только раскрывать, но и использовать определённые сведения определённым способом.
2. Консультант получил эти сведения в рамках договора.
3. Решение второго клиента воспроизводит или применяет именно их.
4. Сходство нельзя объяснить общим профессиональным опытом, независимой разработкой или стандартными отраслевыми практиками.

Если же компания опирается на исключительное право на ноу-хау или на режим коммерческой тайны, к этой лестнице добавляются ещё три ступени: сами сведения не были общеизвестны, имели коммерческую ценность именно из-за секретности, и компания принимала реальные меры защиты.

Первая ступень перекликается с четвёртым пунктом, но смотрит с другой стороны: там речь о том, откуда взялось решение второго клиента, а здесь о том, были ли сами сведения секретом.

А если нужны убытки, а не неустойка, придётся доказать ещё их размер и причинную связь с нарушением.

Чем больше превращений прошли исходные данные по дороге к новому решению, тем слабее причинная связь. Файл стал выводом, вывод соединился с прежним опытом и оформился в принцип, принцип приспособили к другой компании, а та сама внедрила рекомендации.

На каждом шаге появляется альтернативное объяснение результата, и суду мало ощущения, что «без нас он бы до этого не додумался».

Это не значит, что без скопированного файла доказать ничего нельзя. Суд оценивает косвенные доказательства в совокупности: совпадение нетипичных элементов и ошибок, даты, переписку, заключение эксперта. Но каждое звено цепочки придётся собрать.

Развитого аналога доктрины residual knowledge российская практика пока не сформировала, как и устойчивых критериев, отделяющих усвоенное консультантом знание от секрета заказчика. Нет и общепринятой российской версии inevitable disclosure, которая позволяла бы запретить работу с конкурентом только потому, что использование знания кажется неизбежным.

Тем более что в трудовых отношениях даже прямо записанный запрет работать у конкурента после увольнения по общему правилу не применяется, так как ограничивает свободу труда (статья 37 Конституции, часть 2 статьи 9 ТК РФ), и допустимо лишь обязать работника не разглашать коммерческую тайну. [Письмо Минтруда России от 19.10.2017 № 14-2/В-942](#)

С работником NDA вообще работает по другим правилам, чем с внешним консультантом. За разглашение коммерческой тайны работника можно уволить ([подпункт «в» пункта 6 части 1 статьи 81 ТК РФ](#)) и взыскать с него ущерб в полном размере ([пункт 7 части 1 статьи 243 ТК РФ](#)).

Но только прямой действительный ущерб, без упущенной выгоды ([статья 238 ТК РФ](#)), и только если работника заранее под расписку ознакомили с перечнем сведений и режимом тайны ([статья 11 Закона о коммерческой тайне](#)).

А штраф или неустойку, записанные в трудовом договоре или NDA, суды с работника не взыскивают, потому что его ответственность не может быть выше установленной Трудовым кодексом ([часть 2 статьи 232 ТК РФ](#)).

Всё, что в статье говорится о неустойке, относится к договорам с внешними исполнителями.

Иск против консультанта из нашей истории возможен. Просто его судьбу решат конкретный договор и конкретные доказательства, а не моральное чувство собственности на идею, родившуюся в проекте.

Российский NDA защищает прежде всего то, что можно предъявить

Из рассмотренных дел складывается ясная картина. Лучше всего российский NDA работает, когда нарушение оставляет след: файл переслали, доступ открыли, чертёж не вернули, коммерческое предложение ушло от чужого имени, закрытые материалы всплыли в Telegram, продукт изготовили по конкретной документации или клиентам позвонили по переданной базе.

Гораздо хуже, когда нарушение приходится описывать через внутреннее состояние человека: понял принцип, запомнил логику, перенял подход, стал лучше разбираться в отрасли, применил похожую идею, научил другого думать так же.

Заглянуть в голову консультанта и посмотреть там журнал изменений суд не может. Поэтому он ищет внешние проявления: документы, переписку, версии файлов, даты доступа, совпадения, экспертизы, действия на рынке. В этом смысле российский NDA чаще защищает от явного и довольно топорного нарушения.

Не потому, что закон разрешает умное присвоение, а потому, что умное присвоение труднее отличить от законного профессионального роста и ещё труднее доказать.

В России NDA не абсолютный защитный барьер. У него есть вполне юридическая работа: неустойка, распределение рисков, облегчение доказывания. Но не менее важно другое: это договорная инфраструктура доверия, которая задаёт правила поведения, дисциплинирует стороны и создаёт правовые последствия для нарушений, которые можно достаточно уверенно зафиксировать.

Он способен наказать того, кто вынес чертёж, а иногда и того, кто по этому чертежу начал производство. Гораздо хуже он отвечает на вопрос, что делать с человеком, который вернул чертёж, закрыл файл и всё равно запомнил, как устроен механизм.

Значит, следующим шагом должно стать не очередное увеличение штрафа и не расширение понятия конфиденциальной информации до размеров Вселенной, а более разумное устройство самого соглашения. Что должно остаться собственностью клиента, что консультант вправе унести как профессиональный опыт, какие способы использования запрещать, как заранее создать доказательства и почему хороший NDA должен защищать доверие, но не пытаться запретить человеку думать? Об этом заключительная часть.



ЧАСТЬ 4 ИЗ 6

NDA как технология доверия, а не операция по удалению памяти

После всего сказанного может показаться, что составить правильный NDA просто: взять обычный договор, добавить слова «не использовать», увеличить штраф, назвать всю информацию ноу-хау и на всякий случай запретить консультанту работать с отраслью лет десять.

Документ получится внушительный, местами даже пугающий, а работать, скорее всего, будет хуже короткого и разумного соглашения.

Главная беда большинства NDA не в мягкости, а в отсутствии границ. Заказчик пытается объявить своей собственностью всё, что консультант увидел, услышал, понял, разработал, предположил или сможет вспомнить после проекта.

Психологически это понятно: компания открывает постороннему человеку то, что прячет даже от собственных подразделений, и хочет поставить вокруг проекта юридический забор повыше. Только чем выше и шире забор, тем труднее понять, что именно он огораживает.

Если конфиденциальной объявлена «любая информация, ставшая известной в связи с сотрудничеством», вопросы возникают сразу. Относится ли к ней публичная цена на сайте? Вывод консультанта о том, что отдел продаж плохо работает с повторными обращениями? Решение, которое консультант придумал сам, но на основе клиентских данных?

Знание о том, что собственник принимает важные решения только после третьего напоминания? Последнее, возможно, и правда стоит денег, но суду всё равно понадобится более точное описание.

Разумный NDA начинается не с наказания, а с классификации.

Сначала разделить, потом запрещать

До начала проекта сторонам полезно разложить будущие знания и результаты хотя бы по четырём корзинам.

Корзина	Что в неё входит	Кому принадлежит и как используется
Исходная информация клиента	Данные, отчёты, цены, клиентские базы, чертежи, технологии, внутренние решения	Принадлежит клиенту; используется только для согласованной цели
Предшествующие материалы консультанта	Методики, шаблоны, модели, инструменты и подходы, существовавшие до проекта	Остаются у консультанта; клиент получает согласованное право применения
Результаты проекта	Отчёты, модели, регламенты, программные решения и иные созданные материалы	Права определяются договором: передача, лицензия, совместное использование
Обобщённый опыт	Выводы, навыки, профессиональные приёмы и знания, не раскрывающие конкретный секрет	Остаётся у консультанта, если это прописано: закон этот вопрос прямо не решает

На практике корзины пересекаются, поэтому обсуждать их нужно заранее, а не тогда, когда отношения испортились и каждая сторона вдруг вспомнила свою версию происхождения идеи.

Молчание договора о правах здесь не нейтрально. Если отчёт, модель или программу по заказу создаёт консалтинговая компания силами своих сотрудников, исключительное право по умолчанию получает заказчик. [Статья 1296 ГК РФ](#) Если же исполнитель сам автор, например консультант-ИП, который всё сделал лично, это правило не действует.

Право остаётся у него, и чтобы оно перешло к заказчику, это нужно прямо записать, ведь договор, где не сказано, что право передаётся в полном объёме, считается лицензией. [Пункт 3 статьи 1233 ГК РФ](#)

И в любом случае идеи, методы и способы решения задач авторским правом не охраняются, защищены только конкретные тексты, таблицы и код. [Пункт 5 статьи 1259 ГК РФ](#)

Предположим, у консультанта до проекта была модель управления ассортиментом из десяти показателей, а у клиента к ней добавились ещё три, построенные на уникальной экономике его бизнеса. Считать, что вся модель теперь принадлежит клиенту, несправедливо к консультанту.

Считать, что вся она принадлежит консультанту, раз он принёс основу, значит лишить клиента прав на созданное им преимущество. Разумнее оставить исходную методологию консультанту, данные и уникальные параметры клиенту, а права на совместную версию определить отдельно.

Без такого разделения NDA решает вопросы интеллектуальной собственности намёками, а намёками права на коммерчески ценные разработки не распределяют.

Не просто «не использовать», а указать цель

Одна из самых сильных конструкций NDA не абсолютный запрет, а ограничение цели. Информацию передают для диагностики, для подготовки коммерческого предложения, для разработки определённой системы, для оценки возможной сделки или для выполнения конкретного договора, и всё, что выходит за эти пределы, требует отдельного согласия.

Это гораздо точнее общего обещания «не использовать во вред другой стороне». Слово «вред» тянет за собой спор о последствиях и намерениях, а ограничение цели позволяет задать простой вопрос: соответствовало ли действие той задаче, ради которой информацию дали?

Допустим, заказчик передал консультанту клиентскую базу для анализа повторных продаж. Посчитать по ней удержание клиентов можно. Передать подрядчику, который участвует в анализе и связан такими же обязательствами, скорее всего, тоже можно. Предложить этим клиентам собственные услуги нельзя.

Приводить названия компаний как примеры на семинаре можно или нельзя в зависимости от договора и степени обезличивания. А общий вывод о том, что в этой отрасли повторные продажи зависят от скорости обработки рекламаций, скорее всего, допустимый профессиональный опыт, если он не раскрывает конкретных данных и решений заказчика.

Если в такой базе есть ФИО и телефоны покупателей, одного NDA мало: это передача персональных данных. Оформлять её нужно поручением на обработку, где указывают, какие данные, какие действия с ними, зачем и как их защищать, а по букве закона нужно ещё и согласие самих клиентов. [Часть 3 статьи 6 Закона о персональных данных](#)

Перед клиентами за нарушения консультанта отвечает сама компания. Проще всего убрать персональные данные до передачи, если для анализа они не нужны.

Чем яснее определена цель, тем меньше суду придётся заниматься посмертной реконструкцией намерений сторон.

Разглашение и использование в тексте договора

Хорошее соглашение отдельно отвечает на два вопроса: кому и при каких условиях нельзя передавать информацию и для каких действий её нельзя применять, даже никому не передавая. Запрет разглашения охватывает публикацию, пересылку, открытие доступа, устный рассказ, показ документов и передачу материалов третьим лицам.

Запрет использования может касаться извлечения собственной выгоды, работы на прямого конкурента, создания продукта на основе конкретной разработки, обращения к клиентам из переданной базы, воспроизведения внутренних методик, обучения третьих лиц по материалам заказчика и сокращения собственного цикла разработки за счёт полученных результатов.

При этом формулировка не должна запрещать любое применение профессиональных знаний, иначе консультант формально нарушит договор, как только после проекта начнёт лучше писать отчёты или точнее спрашивать. Разумный запрет использования связан с **определённой информацией, определённым действием и определённой целью**.

Что должно остаться у консультанта

Раздел об общих знаниях и профессиональном опыте заказчику редко нравится: кажется, что через эту дверь консультант вынесет из проекта всё, назвав похищенное своей квалификацией. Риск действительно есть, поэтому оговорка не должна звучать как разрешение использовать всё, что удалось запомнить.

Но без неё возникает обратный риск, и клиент получает возможность объявить своей собственностью нормальное профессиональное развитие специалиста.

В договоре полезно прямо признать, что консультант сохраняет право использовать знания и методики, которые были у него до проекта, общедоступную отраслевую информацию и независимо разработанные решения. За ним остаются общие идеи, принципы и навыки, если они не воспроизводят конкретные сведения клиента (обезличивание само по себе этого не гарантирует), профессиональный опыт, не повторяющий конкретных документов, данных, алгоритмов и других охраняемых элементов, и результаты, права на которые остались у него по договору или по закону.

Ограничения записываются рядом. Консультант не вправе намеренно заучивать или воспроизводить закрытые материалы, выдавать конкретную разработку клиента за общий опыт, переносить уникальные параметры, формулы и конфигурации, использовать сведения, по которым можно определить клиента или его стратегию, обходить запрет мелкой переделкой формы и поручать третьим лицам то, что запрещено ему самому.

Граница проходит не между «бумагой» и «памятью», а между **конкретным конкурентным преимуществом клиента** и **обобщённой способностью специалиста решать задачи**.

Не всякое сходство означает кражу

С управленческими методиками нужна особая осторожность. В технических отраслях уникальность решения иногда видна по составу, чертежу, исходному коду или последовательности операций. В консалтинге же многие рекомендации внешне похожи друг на друга: сегментировать клиентов, считать прибыльность по каналам, завести сквозные показатели, сократить цикл принятия решений, поменять систему мотивации, регулярно разбирать отклонения, назначить ответственного за процесс.

Сама рекомендация считать рентабельность по продуктам вряд ли станет ноу-хау. А вот конкретная модель распределения затрат, построенная на уникальных данных и проверенная в определённой бизнес-системе, уже может оказаться охраняемым решением. Поэтому полезно различать уровни сходства.

Сходство	Возможная оценка
Совпала общая управленческая идея	Вероятнее всего, профессиональное или общедоступное знание
Совпала структура модели	Требуется изучить происхождение и степень уникальности
Совпали формулы, параметры и последовательность действий	Возможен перенос конкретного решения
Совпали ошибки, названия, оформление и нетипичные элементы	Сильный признак копирования
Использованы исходные файлы или данные клиента	Наиболее доказуемое нарушение

Иногда лучшее доказательство заимствования не одинаково правильные решения, а одинаково странные ошибки. Это хорошо знают и преподаватели, проверяющие списанные работы, и суды, сравнивающие документы.

Запрет работы с конкурентами должен быть узким

Если заказчик действительно боится, что информацию применят в интересах прямого конкурента, он может попытаться установить специальное ограничение. Но оно должно быть соразмерным, а для этого надо определить, кого считать конкурентом, какую деятельность ограничивать, на какой территории и на какой срок, какие именно сведения создают риск и получает ли консультант компенсацию за существенное ограничение своей работы.

Формулировка «не оказывать любые услуги любым компаниям, работающим в той же отрасли, в течение пяти лет» защищает не столько информацию, сколько рынок от присутствия консультанта. Юридически такой пункт тоже шаток.

Прямого запрета на условие о неконкуренции в договоре с ИП нет, но нет и гарантий: сделки, направленные на ограничение правоспособности гражданина, закон объявляет ничтожными, [пункт 3 статьи 22 ГК РФ](#) а практика по таким условиям неоднородна.

Узкое условие с конкретными клиентами и разумным сроком защитить заметно проще, чем общий запрет работать с отраслью. Исключение сделано для франчайзинга, где закон прямо разрешает обязательство не конкурировать с правообладателем. [Статья 1033 ГК РФ](#)

Особенно сомнительно выглядит запрет, если отрасль и есть основная специализация исполнителя. Нанять специалиста за его опыт, а потом запретить применять этот опыт по специальности — всё равно что пригласить пианиста ради его игры и взять с него обещание больше не садиться за инструмент.

Разумнее ограничивать не саму работу с конкурентами, а конкретные виды проектов и применение конкретных сведений, пока те сохраняют коммерческую ценность. Если же клиенту нужно больше, по сути эксклюзивность консультанта, это отдельный экономический продукт.

Его стоит обсуждать и оплачивать отдельно, а не прятать в пункт о конфиденциальности на семнадцатой странице договора.

У обязательства должен быть срок

Договор без срока или с формулой «бессрочно» для любой информации оставляет открытым вопрос, когда обязанность вообще заканчивается. Для технологии, которая остаётся секретом, это оправдано, для прошлогодних цен и планов на квартал вряд ли.

Разумнее разделить: одни сведения защищаются, пока сохраняют секретность, другие в течение оговорённого числа лет после проекта.

Необходимо перечислить исключения

Хороший NDA описывает не только то, что считается конфиденциальным, но и то, что к этому не относится. Обычно исключают сведения, про которые получатель может подтвердить, что они были общедоступны в момент передачи, стали публичными не по его вине, уже были ему известны на законном основании, получены законно от независимого третьего лица или разработаны самостоятельно без материалов клиента.

Исключают также сведения, которые обязательно раскрывать по закону или предоставлять по мотивированному требованию государственного органа ([статьи 5 и 6 Закона о коммерческой тайне](#)), и те, что обладатель письменно разрешил раскрыть.

Исключения не ослабляют защиту, а делают её определённое. Для раскрытия по требованию закона полезно сразу договориться о порядке: уведомить другую сторону и раскрыть только то, что действительно требуется. Если же договор объявляет тайной даже то, что опубликовано на сайте заказчика, возникает сомнение в серьёзности всего режима.

Защита сильнее у той компании, которая отличает настоящий секрет от привычки ставить гриф «конфиденциально» на каждую презентацию.

Доказательства создаются до нарушения

О доказательствах большинство компаний начинает думать после утечки, и это поздно. Защиту нужно проектировать одновременно с передачей информации. Минимальная система выглядит примерно так:

- перечень категорий конфиденциальных сведений и реестр особо важных документов и моделей;
- маркировка файлов и бумажных носителей с указанием владельца информации;
- разграничение прав доступа и учёт тех, кто получил материалы;
- согласованные каналы передачи, история версий и журналы доступа;
- акты на передачу ключевых комплектов и обязанность сообщать об инцидентах;
- порядок возврата и удаления материалов и подтверждение уничтожения копий после проекта, с оговоркой об автоматических резервных копиях и документах, которые закон обязывает хранить: на них конфиденциальность продолжает действовать;
- доказательства того, что методика существовала до её передачи консультанту.

Последний пункт часто забывают. Чтобы обвинить человека в заимствовании решения, сначала нужно показать, что решение принадлежало компании и существовало в определённом виде до предполагаемого нарушения. Если методика жила в устных разговорах, постоянно менялась и нигде не записана, доказать её содержание и происхождение будет трудно.

Особенно важно фиксировать вклад сторон в совместные разработки. Иначе после успешного проекта заказчик уверен, что всё ценное родилось из его данных, а консультант уверен, что из его интеллекта. Вполне возможно, что оба слегка переоценивают своё участие, как это обычно бывает с авторами успеха.

Когда нарушение обнаружено, фиксировать его нужно сразу. Нотариус составит протокол осмотра страницы сайта, канала или переписки, [статьи 102 и 103 Основ законодательства о нотариате](#) и суд примет его как доказательство, даже если страницу потом удалят.

В деле о 299 чертежах предложения насосов на сайте подрядчика были зафиксированы именно так.

Если нарушение продолжается, решения суда можно не ждать и просить обеспечительную меру, то есть запрет ответчику совершать определённые действия. [Статья 91 АПК РФ](#) Но придётся убедить суд, что без неё исполнить решение станет трудно или компания понесёт значительный ущерб, [статья 90 АПК РФ](#) а такие меры суды принимают осторожно.

Штраф должен помогать, а не украшать договор

Договорная неустойка полезна тем, что избавляет компанию от необходимости доказывать точный размер каждого убытка. [Статья 330 ГК РФ](#) Но из этого не следует, что чем больше сумма, тем надёжнее защита. Если за любое нарушение установлен штраф в 100 миллионов рублей, суд вправе задать разумные вопросы.

Одинаковы ли последствия случайно пересланного письма и переданной конкуренту технологии? Соразмерна ли сумма? Можно ли вообще разделить один случай нарушения от другого? И не пытается ли истец заработать на неустойке больше, чем мог потерять от утечки?

Формально для неустойки между предпринимателями закон допускает снижение лишь в исключительных случаях и только по заявлению должника. На практике, как видно по делам из третьей части, суды снижают договорные штрафы регулярно, и суммы «на вырост» дают для этого самый удобный повод. [Статья 333 ГК РФ](#)

Работоспособнее многоуровневая ответственность: одна сумма за нарушение порядка обращения с информацией, другая за передачу третьему лицу, повышенная за использование в коммерческих интересах и отдельная за публикацию или открытие доступа неопределённому кругу лиц. Туда же стоит записать правило о соотношении неустойки и убытков.

По общему правилу доказанные убытки взыскиваются в части, не покрытой неустойкой, но договор может установить иное: взыскивать только неустойку, взыскивать убытки в полной сумме сверх неустойки или дать пострадавшей стороне выбор между ними. [Статья 394 ГК РФ](#)

Важно заранее определить, что считать одним нарушением, иначе одна сторона будет считать новым эпизодом каждое открытие файла, а другая назовёт всю многомесечную деятельность одним неловким недоразумением. И отдельно оговорить, что штрафы за один и тот же факт

не складываются.

Иначе пересылка файла конкуренту окажется одновременно «нарушением порядка обращения», «передачей третьему лицу» и «использованием в коммерческих интересах», а суд, скорее всего, снизит всю сумму. Размер штрафа должен не поражать воображение, а делать нарушение экономически невыгодным и при этом выдерживать проверку в суде.

NDA должен быть взаимным, когда обмен взаимный

В консультационном проекте уязвим не только клиент. Консультант тоже приносит собственные методики, шаблоны, программные инструменты, базы знаний и способы анализа. Заказчик же порой воспринимает полученные материалы как бесплатное приложение к оплаченным часам: раз файл лёг на корпоративный диск, значит, он теперь наш.

Поэтому взаимное соглашение часто честнее одностороннего. Клиент сохраняет права на свои данные и секреты, консультант на свою прежнюю методологию, права на результат проекта стороны определяют отдельно, и каждая отвечает за разглашение и неправомерное использование чужой информации.

Взаимность меняет и тон переговоров. NDA перестаёт быть документом, которым сильная сторона сообщает слабой «мы вам не доверяем», и становится общим описанием того, как стороны будут обращаться с уязвимостью друг друга.

Что делать самому консультанту

Рассчитывать на то, что клиент ничего не докажет, консультанту мало. Это не профессиональная позиция, а ставка на то, что другая сторона не соберёт доказательств.

Разумная практика начинается с того, чтобы заранее описать собственные методики и материалы и не хранить лишних клиентских данных. Рабочие папки и доступы разных проектов лучше разделять, а материалы между проектами не копировать.

Примеры стоит обезличивать, независимую разработку новых моделей фиксировать, презентации и учебные материалы проверять на клиентские фрагменты, а публичные кейсы согласовывать.

После проекта рабочие копии уничтожаются, кроме резервных копий и того, что положено хранить по закону (на них обязательства сохраняются). Новых клиентов полезно предупреждать о возможном конфликте интересов. Иногда от проекта приходится отказаться, если применить компетенцию, не используя конкретный чужой секрет, действительно невозможно.

Последнее особенно важно. Бывает конфликт, который красивой формулировкой не решить. Если консультант только что помогал одному клиенту разработать стратегию выхода на рынок, а прямой конкурент этого клиента предлагает немедленно разработать встречную стратегию, проблема существует независимо от качества NDA. Профессиональная этика должна начинаться там, где заканчивается вероятность судебного иска.

Доверие не заменяет договор

Фраза «мы доверяем друг другу, поэтому NDA не нужен» звучит благородно, но обычно означает, что стороны по-разному понимают предмет доверия. Один уверен, что консультант никогда не будет работать с конкурентами, другой считает, что будет, просто не станет называть клиента.

Один думает, что созданная методика целиком принадлежит компании, другой, что клиент заплатил лишь за право ею пользоваться. Один полагает, что информацию надо хранить вечно, другой, что через год она устареет.

NDA полезен не тем, что заменяет доверие юридической угрозой, а тем, что заставляет раскрыть содержание этого доверия: что именно доверяют, для чего разрешают использовать, что должно произойти после проекта, какие знания остаются у каждой стороны и что будет считаться предательством договорённости.

В этом смысле хороший NDA похож не на оружие, а на карту минного поля. Риски он не уничтожает, но позволяет заранее увидеть, куда лучше не наступать.

Почему в России NDA ещё и технология доверия

Российское право даёт реальные средства защиты. Можно запретить разглашение и использование, установить неустойку, оформить коммерческую тайну, защищать ноу-хау, требовать возврата документов, прекращения нарушения и возмещения убытков. Но работают эти средства ровно настолько, насколько удаётся превратить знание в определённый объект, а подозрение в доказанную последовательность действий.

В рассмотренных делах суды уверенно наказывали того, кто оставил след: переслал чужое коммерческое предложение, открыл доступ к закрытой системе, не вернул документы, опубликовал внутренние материалы. Преследовать человека, который ничего не копировал, но научился быстрее распознавать проблему и применил это понимание в другом месте, гораздо труднее.

Поэтому настоящая функция NDA одновременно шире и скромнее судебной защиты. Он показывает серьёзность намерений и задаёт нормы поведения, заставляет определить чувствительную информацию и создаёт внутреннюю дисциплину. Он снижает вероятность случайных нарушений, облегчает доказательство очевидных, даёт сторонам язык для разговора о границах и позволяет разойтись без взаимного чтения мыслей.

Но всё это работает, только если за подписью стоят реальные действия: перечень секретов, ограниченный доступ, учёт тех, кто их получил. Без них NDA становится карго-культом: полосу из соломы построили по всем правилам, а самолёты с грузом так и не садятся.

Особенно полезен NDA до конфликта, а после конфликта выясняется только качество ранее проделанной работы.

Договор не должен запрещать человеку измениться

Вернёмся к консультанту, с которого началась статья. Он пришёл в компанию, изучил её данные, увидел скрытые зависимости, помог создать решение и после проекта действительно стал умнее.

Что он вправе унести? Не клиентские файлы, не закрытые цифры и не список покупателей. Не уникальную формулу, не план действий клиента и не модель, права на которую переданы заказчику. А вот способность лучше понимать подобные системы унести вправе, если за ней не прячется конкретный чужой секрет.

Клиент заплатил за решение своей задачи, а не за остановку профессионального развития исполнителя. Консультант получил доступ к чужой уязвимости, а не лицензию превращать её в товар для следующих заказчиков. Между этими двумя утверждениями и должен находиться разумный NDA.

Не юридический забор вокруг чужой головы, не скрытый запрет на профессию и не коллекция штрафов, которую составлял очень рассерженный человек, а соглашение о том, какое конкурентное преимущество одна сторона доверила другой, зачем и где заканчивается чужой секрет и начинается собственный опыт.

NDA не сделает партнёра порядочным, не остановит утечку одним фактом подписи, не гарантирует победы в суде и не вернёт информации секретность после публикации. Но он может заставить стороны заранее договориться о правилах, создать доказательства, отделить ценное от формально засекреченного и поднять цену сознательного нарушения. Для российского бизнеса эта функция не менее важна, чем взыскание неустойки.

NDA защищает не от того, что человек понял. Он защищает от того, что человек сделал с доверенным ему пониманием, а применить у конкурента запомненную чужую формулу значит уже совершить поступок, а не просто понять.

И если соглашение не способно объяснить разницу между этими двумя вещами, перед нами не защита коммерческой тайны, а дорогая письменная просьба вести себя хорошо.



ЧАСТЬ 5 ИЗ 6

NDA и ИИ: третий в комнате

Вернёмся к консультанту из первой части ещё раз. Прошёл год, и у него появилась подписка на облачную модель: Claude, ChatGPT с Codex или Kimi, для нашего разговора это почти неважно.

Тот самый файл с расчётом себестоимости он больше не разбирает вечером с карандашом. Он загружает таблицу в чат и через пару минут получает то, на что раньше уходил день: вот здесь постоянные расходы распределены неверно, и вот насколько это искажает маржу.

Клиент доволен скоростью. Консультант доволен тем, что успевает вести три проекта вместо одного. И возникает вопрос, которого в первых четырёх частях не было: где сейчас этот файл?

Всё сказанное до сих пор упиралось в человеческую память. Знание оседало в голове консультанта, суд туда заглянуть не мог, и NDA защищал в основном от нарушений, которые оставляют следы.

С облачной моделью часть работы мысли переезжает на чужой сервер. Промпт с цифрами клиента, загруженная таблица и ответ модели уже не память, а переписка с третьей компанией. Её хранят, иногда читают, а при случае её может истребовать суд.

Третье лицо, которое не подписывало NDA

Закон о коммерческой тайне называет разглашением ситуацию, когда информация «становится известной третьим лицам» без согласия обладателя. [Пункт 9 статьи 3 Закона о коммерческой тайне](#) Долго было удобно думать об облачной модели как о текстовом редакторе: инструмент, а не собеседник. Появляются первые решения, где думают иначе.

Летом 2026 года Бабушкинский районный суд Москвы признал законным увольнение директора по продажам, которая, среди прочего, выгружала отчёты о сделках и финансах компании в DeepSeek. Суд прямо назвал такую выгрузку разглашением коммерческой тайны.

Решение ещё не вступило в силу, и в деле были и другие эпизоды, например пересылка переписки на личную почту, но формулировка уже прозвучала. [Право.ру о деле № 02-1545/2026, РАПСИ](#)

В США похожая логика сработала против самого обладателя секрета. В январе 2026 года федеральный суд в Калифорнии отклонил иск к OpenAI: истица утверждала, что компания присвоила методики, которые она разработала в диалогах с ChatGPT.

По разбору юрфирмы Foley Hoag, суд рассудил, что, приняв условия сервиса и введя туда сведения, она раскрыла их добровольно и разумных мер охраны не приняла. [Trinidad v. OpenAI, обзор Foley Hoag](#)

Ещё показательнее дело United States v. Heppner, хотя речь в нём об адвокатской тайне, а не о коммерческой: логика та же, всё решают условия сервиса. Бывший топ-менеджер, обвинённый в мошенничестве с ценными бумагами, сам, без поручения адвоката, готовил в потребительской версии Claude документы о стратегии защиты.

В феврале 2026 года судья Ракофф решил, что адвокатской тайны на них нет: модель не адвокат, а условия сервиса допускали и обучение на данных, и раскрытие их по запросу властей. [Разбор McDermott Will & Schulte](#)

Справедливости ради, в ту же неделю суд в Мичигане по похожему поводу пришёл к противоположному выводу, так что практика пока расходится. [Heppner и Warner v. Gilbarco, разбор Jones Walker](#)

Для консультанта из этих дел следует простая вещь. Важен не бренд модели, а условия, на которых он ею пользуется.

Одна модель, разные договоры

Одна и та же модель в личном и в корпоративном тарифе живёт по разным правилам. OpenAI с 2023 года не обучает модели на данных, отправленных через API, если клиент сам не согласился, а логи для контроля злоупотреблений хранит до 30 дней. [OpenAI: как используются данные в API](#)

Бизнес-планы ChatGPT тоже по умолчанию не идут в обучение, а в личных тарифах это решает переключатель в настройках, который нужно не забыть выключить.

Anthropic в августе 2025 года изменила условия для личных тарифов Claude: пользователь сам выбирает, разрешать ли обучение на своих чатах, и если разрешил, данные хранятся пять лет, если нет, тридцать дней.

Корпоративных продуктов и API это не касается. [Anthropic: обновление потребительских условий, Anthropic: обучение на данных коммерческих клиентов](#)

У Kimi картина другая. Китайская редакция политики конфиденциальности прямо говорит, что данные хранятся в КНР, а запросы и ответы могут использоваться для улучшения моделей, и отказаться от этого можно только через обращение в поддержку. [Политика конфиденциальности Kimi](#)

Условия API заключаются с сингапурской компанией, и ограничить использование контента для улучшения сервиса там можно только отдельным корпоративным соглашением. [Условия API Moonshot AI](#)

Отдельная ловушка кроется в словах «я удалил чат». В споре The New York Times с OpenAI суд в мае 2025 года обязал компанию хранить логи ChatGPT, включая удалённые пользователями.

Осенью обязанность хранить новые логи сняли, но выборку из 20 миллионов обезличенных чатов суд велел передать истцам, и в январе 2026 года это решение устояло. [Engadget о приказе хранить логи](#), [National Law Review о 20 миллионах логов](#) Выключенное обучение не означает, что переписки нет на серверах.

Компании поняли это раньше консультантов. В 2023 году инженеры Samsung в нескольких случаях ввели в ChatGPT исходный код и расшифровку внутреннего совещания, после чего компания временно запретила генеративный ИИ на служебных устройствах. [TechCrunch о запрете в Samsung](#), [CIO Dive об утечках](#)

Модель не отвечает за результат. Отвечает тот, кто подписал

Утечка не единственный риск и, как выяснилось, не самый дорогой. В 2025 году Deloitte сдала австралийскому Министерству занятости отчёт стоимостью около 440 тысяч австралийских долларов. Исследователь из Сиднейского университета нашёл в нём ссылки на несуществующие научные работы и выдуманную цитату из решения Федерального суда.

В исправленной версии Deloitte раскрыла, что использовала инструмент на базе GPT-4o, и вернула последний платёж по контракту, около 97 тысяч. [AP о частичном возврате Deloitte](#), [CFO Dive](#)

Самое интересное в этой истории другое. Модель работала в облачной среде самого заказчика, так что с конфиденциальностью, судя по раскрытию, всё было в порядке. Деньги и репутацию компания потеряла не на утечке, а на том, что никто не проверил ссылки.

Через несколько месяцев в Канаде в отчёте Deloitte для провинции Ньюфаундленд и Лабрадор стоимостью почти 1,6 миллиона канадских долларов нашлись четыре несуществующие ссылки. Компания признала ошибки и настаивает на выводах, а провинция в марте 2026 года поменяла правила закупок: подрядчик теперь обязан заранее заявлять, будет ли использовать ИИ, а заказчик вправе это проверять. [CP24 о новых правилах закупок](#), [Fortune](#)

Суды разбираются с тем же уже три года. В 2023 году в Нью-Йорке адвокатов оштрафовали на 5 тысяч долларов за ссылки на решения, которые выдумал ChatGPT, причём суд оговорил, что пользоваться надёжным ИИ само по себе не запрещено, а проверять обязан юрист. [Mata v. Avianca](#)

В 2025 году Высокий суд Англии разобрал иск, где из 45 ссылок 18 вели на несуществующие дела, и предупредил, что общедоступные модели не годятся для надёжного юридического исследования. [Ayinde v Haringey и Al-Haroun v Qatar National Bank](#)

База, которая собирает такие решения по всему миру, к сентябрю 2026 года насчитала больше двух тысяч случаев. [AI Hallucination Cases, база Дамьена Шарлотена](#)

Российские суды догнали мир в 2026 году. Арбитражный суд Западно-Сибирского округа оштрафовал на 50 тысяч рублей компанию, в кассационной жалобе которой были цитаты из несуществующих актов, причём штраф получил клиент, а не юрист. [Гарант о деле № А27-7831/2025](#)

Суд по интеллектуальным правам оштрафовал предпринимателя за жалобу с выдуманной практикой, которую, по словам представителя, подобрал ИИ-сервис правовой базы, и отдельно указал, что за сгенерированный текст отвечает тот, кто применил технологию. [Определение СИП по делу № А71-11377/2025](#)

А 3 сентября 2026 года Верховный суд впервые написал прямо: подготовка позиции с помощью программ идёт на риск стороны и должна сопровождаться проверкой результатов. [Определение СКЭС ВС РФ от 03.09.2026 № 301-ЭС21-23756\(4\)](#)

Для консультанта есть и прямой прецедент. Петербургская компания требовала вернуть деньги за стратегию развития, потому что исполнитель готовил её с помощью нейросети, и заказчик увидел в этом доказательство некомпетентности.

Суд отказал: заказчик подписал акт без претензий и оплатил счёт. [Решение по делу № А56-102880/2024](#) Сам факт использования ИИ основанием для возврата не стал. Но спор возник, и защитил консультанта подписанный акт, а не нейросеть.

Трудоёмкость падает, и цена начинает задавать вопросы

То, что ИИ ускоряет консалтинг, уже не гипотеза. В эксперименте BCG и Гарвардской школы бизнеса 758 консультантов с GPT-4 на подходящих для модели задачах выполнили на 12,2% больше работы, сделали её на 25,1% быстрее и более чем на 40% качественнее.

Сильнее всего подтянулись те, кто изначально работал слабее. [Dell'Acqua et al., Navigating the Jagged Technological Frontier](#)

В том же эксперименте была и задача, которая лежала за пределами возможностей модели. На ней консультанты с ИИ давали верное решение на 19 процентных пунктов реже, чем без него, а оценки качества их рекомендаций при этом были выше.

Ошибка, упакованная моделью, выглядит убедительнее собственной. Для профессии, которая продаёт суждение, это самая неприятная цифра во всём исследовании.

Есть и более бытовая сторона. Исследователи BetterUp Labs и Стэнфорда придумали слово *workslor*: результат, который выглядит как хорошая работа, но не продвигает задачу. 40% опрошенных офисных сотрудников в США получали такое от коллег за последний месяц, и на разбор каждого случая уходило около двух часов. [BetterUp Labs о workslor, Harvard Business Review](#)

Консультант, который отдаёт клиенту черновик модели под своим логотипом, перекладывает эти два часа на клиента и платит за них репутацией.

Когда работа занимает вдвое меньше времени, клиент рано или поздно спрашивает, за что он платит. Американская ассоциация юристов ответила на это ещё в 2024 году. При почасовой оплате можно брать деньги только за реально потраченное время, нельзя выставять клиенту часы на освоение инструмента, а фиксированный гонорар, если ИИ сделал работу намного быстрее, тоже должен остаться разумным.

Там же сказано, что перед вводом сведений клиента в самообучающийся инструмент нужно его информированное согласие, и шаблонной строки в договоре для этого недостаточно. [ABA Formal Opinion 512](#), [обзор The Bar Examiner](#)

Рынок уже движется. У McKinsey около четверти гонораров по миру привязано к результату, а не к часам, и в компании говорят, что ИИ этой модели хорошо подходит. [Business Insider о McKinsey](#)

KPMG, по данным Financial Times, добилась от своего аудитора Grant Thornton снижения гонорара на 14%, прямо требуя поделиться экономией от ИИ. [TheStreet о давлении на аудиторов](#)

В опросе Thomson Reuters треть фирм сокращает долю почасовой работы, а примерно четверть корпоративных юристов уже перевела заказы туда, где предлагают гибкие гонорары. [Thomson Reuters, Future of Professionals 2025](#)

В России этот разговор тоже близко: генеративный ИИ хотя бы в одной функции используют 71% крупных компаний. [Яндекс и «Яков и Партнёры», ИИ в России 2025](#)

Клиент, у которого собственный отдел продаж пишет письма в нейросети, быстро догадается, как устроена часть работы консультанта.

Вывод для цены получается не таким грустным, как кажется. Консультант, который продаёт часы, проиграет, потому что часов станет меньше. Консультант, который продаёт результат и ответственность за него, проигрывает гораздо меньше, потому что проверка, суждение и подпись под выводом никуда не делись. Только честно это работает, если экономию не прячут от клиента.

Российская специфика: персональные данные и договор, которого нет

Российскому консультанту к этому добавляются две вещи, которых у Deloitte не было.

Первая связана с персональными данными. Клиентская база с ФИО и телефонами, о которой шла речь в четвёртой части, в чате ChatGPT, Claude или Kimi означает трансграничную передачу персональных данных.

Такую передачу оператор может начать только после уведомления Роскомнадзора. В страны с адекватной защитой, куда по действующему перечню входят, например, Китай и Сингапур, передача возможна сразу после уведомления, а в остальные, например в США, не раньше, чем ведомство рассмотрит уведомление, и если оно передачу не запретит. [Статья 12 Закона о персональных данных](#), [перечень стран](#), [приказ Роскомнадзора № 128](#)

Критерии перечня закон 2026 года пересматривает, так что статус стран может измениться. [Обзор закона № 265-ФЗ, ppt.ru](#) И уведомление подаёт оператор, то есть обычно сам заказчик, а консультант, получивший базу, работает по его поручению и передавать её дальше без ведома заказчика не вправе.

Обязанность хранить персональные данные россиян в российских базах действует с 2015 года, а с 1 июля 2025 года закон прямо запрещает при сборе записывать и хранить их в иностранных базах. [Часть 5 статьи 18 Закона о персональных данных](#)

Утечка может обойтись компании от 3 до 15 миллионов рублей в зависимости от числа затронутых людей, а повторная до 3% годовой выручки. [Статья 13.11 КоАП РФ](#)

Вторая связана с тем, что договора часто просто нет. России нет в списках стран, где официально работают OpenAI и Anthropic. [OpenAI: поддерживаемые страны](#), [Anthropic: поддерживаемые страны](#)

Значит, корпоративный тариф с обязательством не обучаться на данных российский консультант не оформит, не нарушив условий самих провайдеров, а личный аккаунт через VPN эти условия нарушает и может быть заблокирован.

Совет «пользуйтесь бизнес-версией» в российских условиях звучит примерно как совет купить страховку в компании, которая не продаёт полисы в вашей стране.

Государство тем временем выбрало свою линию. Закон от 26 июля 2026 года № 243-ФЗ о поддержке развития технологий искусственного интеллекта, действующий с 1 сентября, вводит понятия суверенных и национальных моделей и позволяет правительству определять сферы, где допускаются только они.

По опубликованным обзорам, ограничения для зарубежных моделей из итоговой версии закона убрали, так что прямого запрета для частного консультанта нет. [Федеральный закон № 243-ФЗ, обзор ppt.ru](#)

Если же клиент работает с критической инфраструктурой или в госсекторе, вопрос о зарубежном облачном ИИ лучше задать его юристам до начала проекта.

Российские альтернативы для чувствительных данных существуют. GigaChat API, по условиям Сбера, по умолчанию не хранит запросы и не использует их для дообучения, а данные обрабатываются на серверах в России. [GigaChat API](#)

Yandex AI Studio, наоборот, по умолчанию запросы логирует, но это отключается, и сам Яндекс советует так делать при передаче конфиденциальных сведений. [Yandex AI Studio: отключение логирования](#) У обеих компаний есть варианты, которые работают внутри контура заказчика.

Профессиональные сообщества пока советуют, а не требуют. Банк России в кодексе этики ИИ для финансового рынка рекомендует сообщать клиентам о взаимодействии с ИИ. [Кодекс этики Банка России в сфере ИИ](#)

Вице-президент Федеральной палаты адвокатов говорит, что применять ИИ к материалам доверителя стоит только по согласованию с ним. [РАПСИ, позиция ФПА](#) Для консультанта логика та же.

Третий в комнате

Вся эта статья держалась на одной мысли: NDA защищает не от того, что человек понял, а от того, что он сделал с доверенным ему пониманием. Облачная модель эту мысль не отменяет, но добавляет в неё действующее лицо. Часть понимания консультант теперь арендует у компании, которая не подписывала NDA, живёт по своим условиям и иногда по законам другой страны.

Запрещать консультанту ИИ, скорее всего, бесполезно: такой запрет плохо проверяется, а работа без моделей становится заметно дороже. Разумнее договориться, какой ИИ, в каком режиме и с какими данными допустим. Что именно уходит провайдеру, когда консультант работает в чате и когда запускает агента на своём компьютере, как обезличивать данные и какое условие о разрешённом использовании ИИ записать в NDA, разберём в шестой части.

Раньше клиенту было достаточно доверять консультанту. Теперь ему нужно знать, кому консультант доверяет сам.



ЧАСТЬ 6 ИЗ 6

Разрешить, но с условиями: как консультанту работать с ИИ под NDA

Консультант из пятой части прочитал про логи ChatGPT и выдуманные ссылки Deloitte и сделал вывод. Таблицы клиента в чат он больше не загружает. Теперь у него агент: программа запускается на его компьютере, в папке проекта, сама открывает файлы, пишет расчётную модель и считает.

«Файлы же лежат у меня на диске», говорит он клиенту. И это правда. Вопрос в том, что при этом всё-таки уходит наружу.

Чат и агент: что на самом деле уходит

Главная поправка к интуиции проста: модель по-прежнему работает в облаке. Агент на ноутбуке только посредник, а думает сервер провайдера. Значит, на сервер уходит всё, что агенту понадобилось показать модели.

Документация Claude Code описывает это прямо. По сети отправляются промпты пользователя и ответы модели, а в контекст модели попадают история разговора, содержимое прочитанных файлов и вывод выполненных команд. [Claude Code: как используются данные, как устроен Claude Code](#)

Выгружать проект целиком агент не обязан. Он ищет нужные файлы и читает их. Но всё, что он открыл, и всё, что вывел на экран скрипт, модель увидела, а значит, и провайдер получил.

У OpenAI то же разделение. Локальный Codex CLI выполняет команды на компьютере пользователя, а в облачном режиме Codex создаёт контейнер на серверах OpenAI и выкачивает туда репозиторий.

Состояние такого контейнера хранится до 12 часов. [Codex: облачная среда](#), [справка OpenAI о локальном и облачном Codex](#)

У Kimi тоже есть агент для терминала, Kimi Code CLI. [Kimi Code на GitHub](#) Отдельного документа о данных для него найти не удалось, а общие условия Kimi говорят о хранении в КНР и использовании запросов для улучшения моделей. [Политика конфиденциальности Kimi](#)

Есть и то, что остаётся на компьютере, но само становится риском. Claude Code по умолчанию 30 дней хранит транскрипты сессий открытым текстом в папке пользователя, а туда попадает всё, что прошло через инструменты агента. [Claude Code: папка .claude](#) Украденный ноутбук консультанта превращается в архив чужих секретов.

Есть и неочевидные каналы. Если отправить разработчику отчёт об ошибке через встроенную команду обратной связи, копия переписки вместе с кодом хранится у Anthropic пять лет. Внешние подключения к сервисам, так называемые MCP-серверы, Anthropic не проверяет, и данные уходят их владельцам. [Claude Code: безопасность](#), [Claude Code: MCP](#)

Если свести всё вместе, картина выглядит так.

Режим	Что получает провайдер модели	Что остаётся у консультанта	Что может уйти третьим лицам
Чат	Загруженный файл и переписку	Оригинал файла	Поисковику и подключённым сервисам
Локальный агент	Всё, что агент прочитал и увидел: фрагменты файлов, вывод команд	Остальные файлы и локальные журналы сессий	Внешним подключениям, поисковику, сайтам, злоумышленнику через внедрённую инструкцию
Облачный агент	Копию проекта целиком	Оригинал	То же, что у локального агента
Локальная модель или сервис в контуре заказчика	Ничего, либо российский провайдер по договору	Всё	Только то, что сознательно подключено

Код к данным, а не данные к модели

Из этой таблицы вытекает приём, который серьёзно снижает риск. Модели не нужно видеть клиентскую базу, чтобы написать скрипт, который её посчитает. Ей достаточно структуры таблицы и нескольких выдуманных строк.

Схема получается такая. Агент видит описание полей и синтетический пример, пишет код, код запускается локально на настоящих данных, а модель получает только итоговые цифры: сколько клиентов вернулось, какая маржа по каналам, где ошибка в распределении затрат.

Честности ради: ни Anthropic, ни OpenAI такой рецепт в своей документации прямо не предлагают, это практика, а не официальная рекомендация. Близкий аналог давно работает в медицинской статистике.

В проекте OpenSAFELY исследователи пишут код на фиктивных данных, а выполняется он внутри защищённой среды с настоящими медицинскими записями. [OpenSAFELY: документация](#)

У приёма есть предел. Итоговые цифры и сообщения об ошибках тоже попадают в контекст модели. Если скрипт упал и напечатал первую строку таблицы с фамилией покупателя, эта фамилия ушла на сервер.

Поэтому агенту нужно прямо запрещать смотреть сырые данные, а скрипты писать так, чтобы они печатали только агрегаты.

Запрет чтения папки в настройках агента помогает, но не абсолютно. Документация Claude Code сама предупреждает, что такой запрет не мешает скрипту на Python открыть файл самостоятельно.

Жёсткую изоляцию даёт песочница, а на обычном Windows её нет, только через подсистему Linux. [Claude Code: права доступа](#), [Claude Code: песочница](#)

Чем агент опаснее чата

У агента больше возможностей, и в этом его главный риск. Чат видит то, что вы в него вставили. Агент видит всё, до чего дотянется на диске, умеет выполнять команды и ходить в интернет.

OWASP, некоммерческое сообщество по безопасности приложений, ставит на первое место среди рисков языковых моделей внедрение инструкций: модель выполняет команду, спрятанную в файле, письме или на веб-странице.

Рядом стоят утечка чувствительной информации и избыточные полномочия агента. [OWASP Top 10 для LLM-приложений 2025](#)

Это не теория. В 2025 году исследователь показал, что инструкция, спрятанная в файле проекта, могла заставить Claude Code отправить ключи доступа наружу через обычные сетевые запросы, которые агент считал безопасными. Anthropic уязвимость исправила. [Advisory CVE-2025-55284, разбор исследователя](#)

В том же году похожая по сути атака на Microsoft 365 Copilot получила оценку опасности 9,3 из 10: достаточно было прислать письмо, чтобы ассистент выдал данные пользователя. [Microsoft: CVE-2025-32711, статья исследователей EchoLeak](#)

OpenAI в документации Codex приводит показательный пример: инструкция в описании задачи на GitHub заставляет агента отправить свежие изменения кода на чужой сервер, если у агента включён интернет. [Codex: доступ в интернет](#)

Для консультанта отсюда следует несколько привычек. Агента, который работает с данными клиента, лучше держать без интернета и без лишних подключений. Выполнение команд подтверждать вручную. Чужие файлы и страницы, которые агент читает, считать потенциально враждебными.

А телеметрию и отправку отчётов с транскриптами отключить, благо в документации для этого есть отдельные настройки. [Claude Code: как используются данные](#)

Не запрещать, а разрешить с условиями

Первая реакция клиента на всё это понятна: запретить. Проблема в том, что запрет плохо проверяется. Автор разбора в «Т-Бизнес секретах» пишет прямо: полный запрет сотрудники обходят, и работает не запрет, а политика с разрешёнными сервисами, обезличиванием и контролем. [«Утечки данных через ИИ: почему запреты не спасают бизнес»](#)

Профессиональные сообщества приходят к тому же. Английская юридическая ассоциация советует выяснять, обучается ли инструмент на введённых данных, читать условия каждого сервиса и заранее планировать выход с удалением данных. [Law Society: Generative AI, the essentials](#)

Британский институт бухгалтеров ICAEW прямо рекомендует не загружать конфиденциальную информацию в публичные инструменты генеративного ИИ и говорить клиенту, если ИИ участвовал в анализе. [ICAEW: Generative AI guide, Ethics](#)

Американская ассоциация юристов требует информированного согласия клиента до ввода его сведений в самообучающийся инструмент. Клиенту нужно объяснить, зачем используется инструмент, какие данные в него попадут и чем это рискованно, а шаблонной строки в договоре недостаточно. [Обзор ABA Formal Opinion 512](#)

Самый конкретный образец дало правительство Австралии. В его типовых условиях об ИИ исполнитель обязан до использования ИИ в услугах уведомить заказчика и получить письменное одобрение. Загружать данные заказчика в языковые модели запрещено, если договор прямо этого не разрешает. [AI Model Clauses Агентства цифровой трансформации Австралии, копия PDF](#)

Американский институт стандартов NIST в профиле рисков генеративного ИИ советует вести утверждённый перечень ИИ-инструментов и провайдеров и прописывать в договорах права на оценку того, как третьи лица используют ИИ. [NIST AI 600-1](#)

Российские юристы предлагают удобную рамку: разделить сведения на классы. Одни не уходят ни в какой ИИ, другие только в корпоративные решения, третьи куда угодно. [«Коммерческая тайна и ИИ», Т-Бизнес секреты](#)

На Право.ру к этому добавляют обязательную проверку результата и порядок действий при утечке через промпт. [«Политика работы с ИИ», Право.ру](#)

Для российского консультанта в эту рамку приходится внести поправку из пятой части. Корпоративный тариф OpenAI или Anthropic с гарантией «не обучаем» ему не оформить, не нарушив условий самих провайдеров, а режим нулевого хранения данных провайдеры дают только одобренным корпоративным клиентам. [Claude Code: нулевое хранение данных](#)

Поэтому «разрешённый инструмент» для сведений второго класса на практике означает российский корпоративный сервис, среду самого заказчика или локальную модель. GigaChat API, по условиям Сбера, по умолчанию не хранит запросы и не дообучается на них. [GigaChat API](#)

В Yandex AI Studio хранение запросов нужно отключить явно. [Yandex AI Studio: отключение логирования](#)

Обезличивание: где проходит граница

Обезличивание выглядит простым решением: убрал фамилии, и можно работать. На деле с ним связаны три неприятных вопроса.

Первый вопрос юридический. Закон называет обезличиванием действия, после которых нельзя определить, кому принадлежат данные, без дополнительной информации. [Пункт 9 статьи 3 Закона о персональных данных](#) Раз у кого-то есть ключ, данные можно восстановить.

Остаются ли такие данные персональными, в России единого ответа нет. Представители Роскомнадзора на встрече с бизнесом в 2025 году говорили, что обезличенные данные всё равно персональные, в том числе для требований о локализации. [Birch Legal о позиции Роскомнадзора](#)

Юристы Контура считают иначе: обезличенные данные теряют связь с человеком и под определение уже не попадают. [Контур: обезличивание персональных данных](#)

Пока спор не решён, безопаснее исходить из позиции регулятора. Обезличенная клиентская база в зарубежном чате остаётся вопросом трансграничной передачи. [Статья 12 Закона о персональных данных](#)

В Европе логика похожая: псевдонимизированные данные по общему правилу остаются персональными. [GDPR, вводное положение 26 и статья 4](#) Суд ЕС в сентябре 2025 года добавил важную оговорку: для получателя, у которого нет ключа и нет разумной возможности установить человека, такие данные могут и не быть персональными. [Суд ЕС, EDPS v SRB, пресс-релиз](#) Отправитель же, у которого ключ остался, свою ответственность не теряет.

Второй вопрос технический: как обезличивать. С 1 сентября 2025 года действует приказ Роскомнадзора № 140, который заменил прежний приказ 2013 года. Он называет четыре метода: замену значений кодами с таблицей соответствия, изменение состава данных, перемешивание и разделение массива на части. [КонсультантПлюс о приказе Роскомнадзора № 140](#)

Там же есть требования, которые полезно перенести в договор. Обезличенные данные нельзя хранить вместе с исходными, а действия по обезличиванию нужно учитывать. [Обзор требований приказа № 140](#)

Для консультанта это переводится просто: таблица «клиент 0147 = ООО „Ромашка“» остаётся у заказчика или в отдельном месте, куда агент не ходит.

Автоматические помощники есть, но полагаться на них целиком нельзя. Microsoft Presidio находит и маскирует персональные данные в тексте, однако из коробки работает с английским, а для русского ему нужны отдельные модели.

Сам проект предупреждает, что находит не всё. [Microsoft Presidio, поддержка языков в Presidio](#) Для русского текста есть открытая библиотека Natasha, которая распознаёт имена, места и организации. [Natasha](#)

Третий вопрос самый неприятный: обезличенное не значит неузнаваемое. Ещё в 2000 году исследовательница Латания Суини показала, что 87% жителей США однозначно определяются по почтовому индексу, полу и дате рождения. [Sweeney, Simple Demographics Often Identify People Uniquely](#)

Языковые модели делают эту задачу ещё проще. Исследование 2024 года показало, что модели угадывают по обычному тексту место жительства, доход и другие признаки автора с точностью до 85%, и стандартное обезличивание текста от этого не защищает. [Staab et al., Beyond Memorization](#)

Поэтому кроме фамилий приходится обобщать косвенные признаки: вместо даты рождения возрастная группа, вместо адреса регион, вместо точной суммы диапазон.

И наконец, главная оговорка для NDA. Обезличивание защищает персональные данные, но почти не защищает коммерческую тайну. Если из отчёта убрать название клиента, цифры его сделок, маржа по каналам и план выхода в новый регион останутся секретом.

А конкурент, знающий рынок, узнает компанию по трём цифрам быстрее любой модели.

Условие о разрешённом использовании ИИ

Всё сказанное можно собрать в отдельное условие NDA или договора. Это не готовый юридический шаблон, а перечень того, о чём сторонам стоит договориться заранее:

- **Перечень инструментов.** Приложение к договору называет разрешённые сервисы и режимы: российский корпоративный сервис, среду заказчика, локальную модель. Бесплатные и личные версии зарубежных моделей допустимы только для сведений, которые можно было бы опубликовать.
- **Запрет обучения.** Сведения заказчика не используются для обучения и дообучения моделей. Исполнитель подтверждает настройки датированными доказательствами: снимками настроек и версией условий сервиса на дату работ. Перечень разрешённых сервисов пересматривается, когда провайдер меняет условия, а личный аккаунт, открытый в обход условий сервиса, разрешённым инструментом не считается.
- **Классы сведений.** Для каждой категории указано, куда её можно отправлять: никуда, только в разрешённые инструменты или без ограничений.
- **Роли и обезличивание.** Заказчик как оператор персональных данных даёт консультанту поручение на обработку ([часть 3 статьи 6 Закона о персональных данных](#)), где сказано, кто и какими методами обезличивает данные и кто отвечает за качество. Таблица ответственности хранится отдельно и не передаётся в ИИ. Метод из приказа Роскомнадзора сам по себе результат не гарантирует, поэтому после обезличивания проверяется, нельзя ли узнать человека по оставшимся признакам. Уведомление о трансграничной передаче подаёт оператор, и без его решения консультант данные в зарубежные сервисы не передаёт.
- **Правила для агентов.** Агент работает без доступа в интернет и без внешних подключений, не читает сырые данные без необходимости, отправка транскриптов провайдеру отключена, локальные журналы удаляются.
- **Согласие на конкретный инструмент.** До начала работ исполнитель сообщает, какой инструмент, для каких задач и с какими категориями данных будет использован, а заказчик одобряет это письменно. Такое одобрение договорное: законного основания для обработки персональных данных оно не заменяет.
- **Проверка и ответственность.** Каждый результат, полученный с участием ИИ, проверяет человек, и исполнитель отвечает за него как за собственную работу.

- **Прозрачность.** По запросу заказчика и обязательно для ключевых выводов исполнитель раскрывает, где применялся ИИ.
- **Контроль и санкции.** Заказчик вправе запросить журнал использования ИИ и подтверждения настроек. Требования распространяются на субподрядчиков и помощников исполнителя. Разрешается конкретная конфигурация агента и перечень его подключений, а не просто название сервиса. За использование неразрешённого сервиса предусмотрена неустойка.
- **Инциденты.** Об ошибочном вводе сведений в неразрешённый сервис исполнитель сообщает немедленно. Если затронуты персональные данные, заказчик как оператор обязан уведомить Роскомнадзор в течение 24 часов, а о результатах расследования в течение 72 часов, поэтому время на сообщение у консультанта измеряется часами. [Часть 3.1 статьи 21 Закона о персональных данных](#)
- **Выход.** После окончания проекта исполнитель удаляет то, что контролирует: историю чатов, аккаунты проекта, рабочую среду агента. Журнал действий хранится зашифрованным оговорённый срок на случай разбирательства и потом удаляется. Удалить данные на стороне провайдера можно только в пределах его условий, поэтому исполнитель фиксирует, какие сведения и в какой сервис вводились.

К этому перечню стоит добавить права на результат. В четвёртой части говорилось, что молчание договора о правах не нейтрально, а с ИИ появляется ещё один слой: российские суды охраняют результат, в котором виден творческий вклад человека, и продолжают спорить о том, где этот вклад начинается.

Дипфейк-ролик признали охраняемым, потому что за ним стояли сценарий, съёмка и звук. [Дело № А40-200471/2023, IPC Magazine](#) А в споре о картинках, которые первая инстанция сочла сделанными нейросетью, Мосгорсуд в августе 2026 года решение отменил. [РАПСИ о деле «Мона Лиза с вином»](#)

Заказчику, который платит за модель или стратегию, спокойнее, когда договор прямо говорит, кому принадлежит результат, и не зависит от того, как суд оценит долю машины. Но если творческого вклада человека в результате нет, договор не делает его объектом исключительного права. Тогда защищать результат приходится договорными средствами: режимом конфиденциальности и обязательством не использовать и не разглашать.

Последний пункт касается цены. Экономия от ИИ лучше не прятать. Американская ассоциация юристов запрещает брать почасовую оплату за время, которое сэкономят инструмент. [ABA Formal Opinion 512](#)

Для консультанта честнее продавать результат с понятными критериями приёмки и заранее говорить, какую часть работы делает модель.

Договор, который называет третьего по имени

Шестая часть получилась самой практической, но держится на той же мысли, что и вся статья. NDA защищает не от того, что человек понял, а от того, что он сделал с доверенным ему пониманием.

Облачная модель добавила в эту формулу третье лицо, а агент сделал его ещё и активным участником, который сам читает файлы и выполняет команды. Запретить его бесполезно, а игнорировать опасно.

Остаётся договориться: какой ИИ, в каком режиме, с какими данными и под чью ответственность.

Такой договор длиннее прежнего на пару страниц. Зато он честно отвечает на вопрос, который клиент рано или поздно задаст: кто ещё видел мои цифры?

Где читать и смотреть дальше

Статья выходила частями в Дзене, и я читаю её вслух на видео. Первая часть открыта для всех: [текст в Дзене](#), видео на [YouTube](#), [RUTUBE](#) и [VK Видео](#).

Новые статьи и разборы выходят в каналах:

Telegram-канал @ab_dublin

статьи и материалы

Telegram-канал @friday_meb

пятничные посты для собственников мебельных фабрик

Дзен · dzen.ru/db/dubas

«Филистер филистерам. Записки антрополога бизнеса»

YouTube

«Филистер филистерам | Александр Борисович»

RUTUBE

«Александр Борисович Дублин | Системный бизнес»

ВКонтакте и VK Видео · @ab.dublin

«Александр Борисович Дублин | Системный бизнес»

Книги автора

«Мебельщикам в кризис»

Шестнадцать разговоров о том, что делать

«Мебель и коньяк»

Истории о мебельном интернет-бизнесе

«Склад незавершёнки»

Как управлять воронкой продаж в мебели на заказ

«Два этажа продаж»

Как управлять РОПом

«Вредные советы»

Руководство по обману покупателя мебели на заказ

«Разори мебельщика!»

Вредные советы покупателю мебели

Все книги — на странице автора на Литресе: litres.ru/author/aleksandr-dublin

НАПИСАТЬ АВТОРУ

Александр Борисович Дублин, аналитик бизнеса, консультант, ментор

Telegram: [@AleksandrBorisovich73](https://t.me/AleksandrBorisovich73)

Телефон и WhatsApp: [+7 921 751-59-28](https://wa.me/79217515928) (Telegram на этом номере нет)