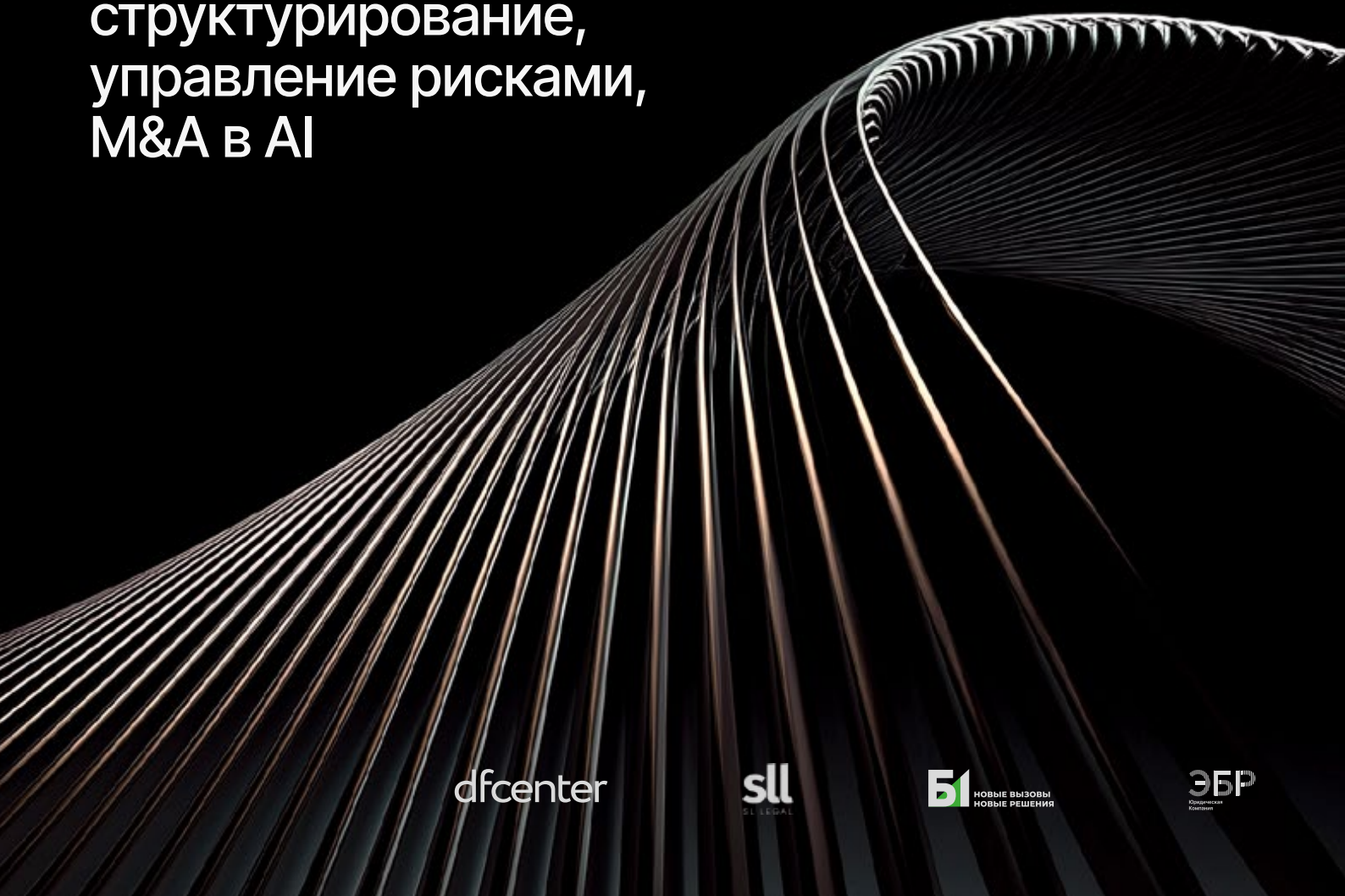
АНАСТАСИЯ НЕРЧИНСКАЯ | VERBA LEGAL | АЛРУД | Dénuo | ADVANCE CAPITAL

Tech M&A 2025

ЧАСТЬ 2

Due diligence, структурирование, управление рисками, M&A в AI



dfcenter | sll | НОВЫЕ ВЫЗОВЫ НОВЫЕ РЕШЕНИЯ | ЭБР Юридическая Компания

Хедлайнеры исследования выражают искреннюю благодарность всем участникам, присоединившимся к подготовке материала Части 2. Tech M&A 2025. Due diligence, структурирование, управление рисками, M&A в AI.

BETTER CHANCE

ELWI

KAMA FLOW

KKMP LEGAL

LEVEL Legal Services

Melling Voitishkin &Partners

NEXTONS

NIKOLSKAYA consulting

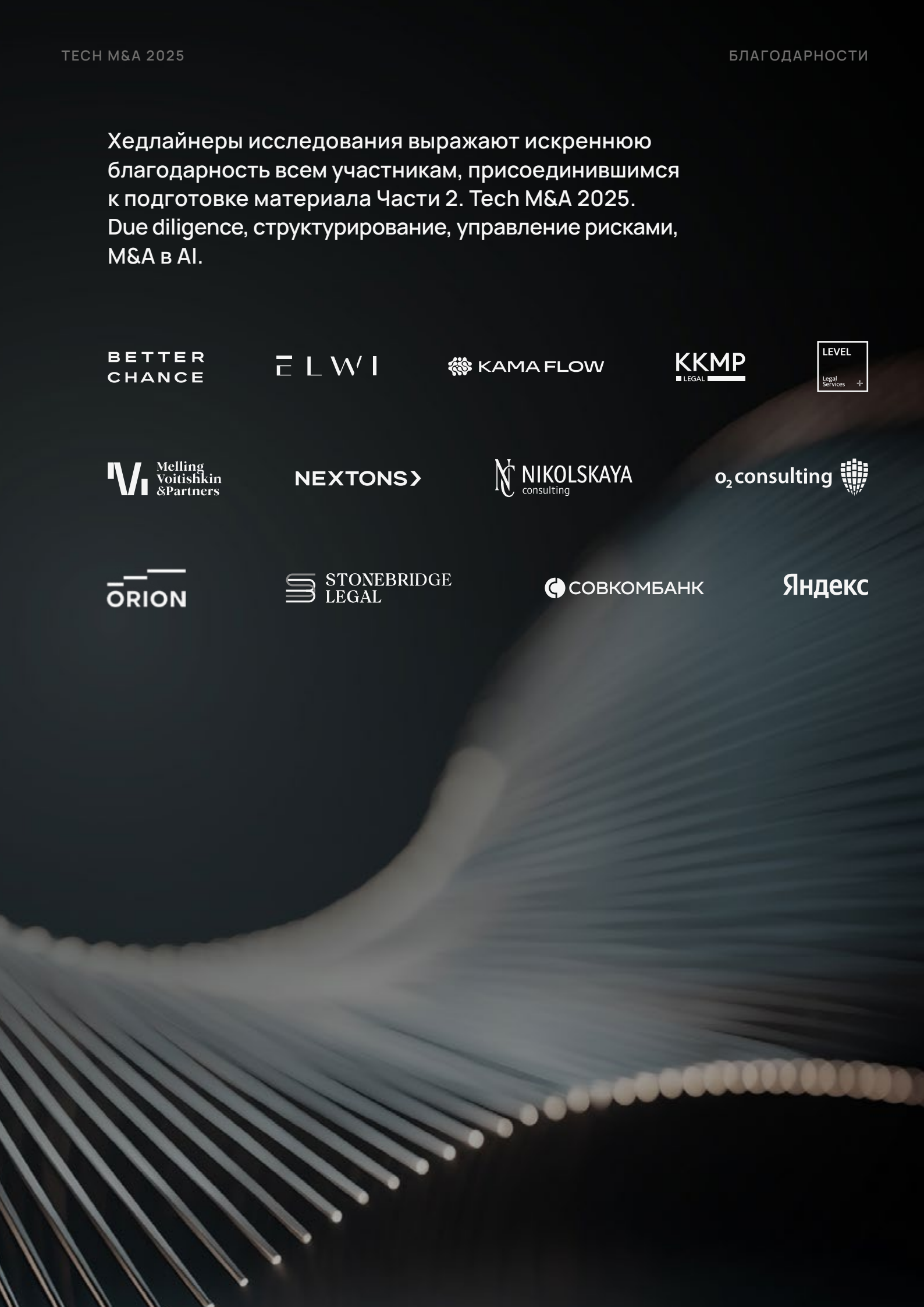
O_2 consulting

ORION

STONEBRIDGE LEGAL

СОВКОМБАНК

Яндекс



1

Особенности юридического структурирования сделок Tech M&A 2025

7

01 Tech M&A активность 2025 8

02 Структуры и форматы сделок Tech M&A в 2025 г. 32

03 Структурирование и управление рисками в сделках с технологическими активами 54

04 Спецпроект: earn-out — решение проблемы или иллюзия договоренности 155

2

Due Diligence и управление рисками в сделках Tech M&A

163

01 Области проверки и ключевые риски IT-компаний 164

02 Подходы к митигации юридических IT-рисков 233

03 Юридический due diligence программных продуктов 305

04 Техническая экспертиза в сделках Tech M&A 354

3

Юридическая специфика сделок M&A с ИИ-компаниями

385

01 Периметр ключевых активов ИИ-компаний в контексте M&A 386

02 Due diligence и ключевые риски ИИ-бизнесов 454

03 Распределение ИИ-специфических рисков между сторонами сделки M&A 543

Приложения

01 Используемые термины 595

02 Методология исследования 600

03 Корпоративные хедлайнеры исследования 608

04 Ограничение ответственности 622

Уведомление об авторских правах

Правообладатели исследования:
Анастасия Нерчинская, DENUO, АЛРУД, VERBA LEGAL

Права на подбор и расположение материалов исследования принадлежат Анастасии Нерчинской

Исследование организовали и провели Анастасия Нерчинская, DENUO, VERBA LEGAL, АЛРУД и ADVANCE CAPITAL.

Использование

Использование какой-либо части данного исследования допускается **исключительно в некоммерческих целях** (информационных, научных, учебных или культурных) **в формате цитирования** в объеме, оправданном целью цитирования. Полное или частичное воспроизведение текста, структуры, аналитических выводов и данных исследования **в коммерческих целях запрещено без предварительного письменного разрешения всех трех правообладателей**.

Цитирование

При цитировании какой-либо части исследования в любой объективной форме, будь то текст, графики или данные опросов, воспроизведение и исполнение, включая использование содержащейся в исследовании информации, **обязательна ссылка на данное исследование** в качестве источника цитаты с указанием правообладателей, хедлайнеров и названия исследования в следующем формате:

«Tech M&A 2025. Часть 2. Due diligence, структурирование, управление рисками, M&A в AI, организованное и проведенное Анастасией Нерчинской, DENUO, АЛРУД, VERBA LEGAL и ADVANCE CAPITAL».

В случае цитирования исследования при размещении материалов в Интернете (сайты, телеграм-каналы, социальные сети и т. п.) также обязательно **указание прямой активной гиперссылки** на источник публикации.

© 2026 Анастасия Нерчинская, DENUO, VERBA LEGAL, АЛРУД. Все права защищены.

Правообладатели исследования: Анастасия Нерчинская, DENUO, АЛРУД, VERBA LEGAL

Права на подбор и расположение материалов исследования принадлежат Анастасии Нерчинской

Устные выступления

При цитировании фрагментов исследования в устном выступлении, помимо указанных выше, обязательна ссылка на исследование в устной форме сразу по окончании цитирования.

Права третьих лиц

Информация об авторах внешних комментариев указана в тексте исследования. Цитирование авторских комментариев допускается только при условии указания информации об авторах используемых комментариев, а также ссылки на данное исследование в указанных выше форматах. Все товарные знаки, упомянутые в исследовании, принадлежат их правообладателям.

Ответственность

Какое-либо использование материала, за исключением цитирования с учетом указанных выше требований, запрещено и будет являться нарушением авторских прав.

Авторы комментариев, приведенных в данном исследовании, гарантируют их оригинальность и самостоятельно несут ответственность за соблюдение прав третьих лиц при подготовке таких комментариев. Мнение правообладателей исследования может не совпадать с мнением авторов комментариев, приведенных в исследовании.

© 2026 Анастасия Нерчинская, DENUO, VERBA LEGAL, АЛРУД. Все права защищены.

Об исследовании

Уважаемые читатели!

Мы рады представить вашему вниманию вторую часть масштабного экспертно-аналитического исследования, посвященного вопросам юридического структурирования сделок с технологическими компаниями в российском сегменте TMT.

В силу отраслевой специфики сделки M&A в tech-индустрии всегда отличались сложным юридическим структурированием независимо от ценового сегмента приобретаемых активов. В 2025 г. рынок Tech M&A перешел в более зрелую фазу, общий вектор транзакционной активности сместился в сторону точечного входа инвесторов в проекты поздних стадий, подтвердивших устойчивость в условиях высокой неопределенности. Несмотря на снижение общего количества таких сделок в сравнении с предыдущими периодами, процесс их структурирования в 2025 г. существенно усложнился. Продавцы качественных активов менее охотно уступали позиции по ценовым условиям, поиск компромисса по ключевым параметрам сделок стал более длительным и напряженным, а юристам чаще приходилось искать гибкие и нестандартные решения.

Представленный материал состоит из трех крупных частей. Первая глава включает детальный обзор трендов и анализ особенностей структурирования сделок Tech M&A в 2025 г. В ходе ее подготовки мы попросили ведущих M&A-консультантов и транзакционные команды крупных игроков рынка рассказать о своем опыте сопровождения наиболее сложных и знаковых сделок в 2025 г., отметить проблемные вопросы, на которых фокусировались стороны, и поделиться стандартами лучших практик транзакционной работы, адаптированных к текущим бизнес-реалиям и новому инвестиционному ландшафту. В первой главе исследования отражен системный взгляд на механики распределения рисков, подходы к структурированию расчетов и выбору переговорных стратегий, актуальные в 2025 г.

Во второй главе мы обобщили многолетний опыт хедлайнеров и участников исследования в области due diligence программных продуктов, являющихся ключевыми активами многих технологических компаний. На основе обзора мнений ведущих экспертов мы систематизировали наиболее значимые выявляемые риски, рассказали о распространенных заблуждениях, которые могут привести к серьезным ошибкам при анализе прав на ПО и другие IT-активы, и поделились мнением о том, как эффективно выстроить процесс юридической проверки в сжатые сроки.

Третью главу материала мы посвятили вопросам юридического структурирования сделок M&A с принципиально новым типом активов, в основе которых лежат ИИ-технологии. Стремительное развитие генеративного ИИ ставит перед M&A-юристами серьезные задачи и требует переосмысления классических подходов к структурированию Tech M&A сделок, которые не всегда эффективны при работе с ИИ-активами. Предлагаемый читателям материал является первой и уникальной попыткой комплексного исследования наиболее сложных вопросов, возникающих при структурировании сделок с ИИ. Мы провели всесторонний и глубокий анализ аспектов, связанных с формированием периметра ключевых активов ИИ-бизнесов, определением их правового режима, проведением due diligence ИИ-моделей, систем и датасетов, механиками распределения ИИ-специфических рисков и их митигацией.

Мы надеемся, что это исследование будет для вас полезным. Благодарим за ваше внимание и желаем приятного чтения!

Авторы исследования

1

Особенности юридического структурирования сделок Tech M&A 2025



Раздел 1

Tech M&A активность 2025

Взгляд ведущих игроков

АВТОРЫ



Анастасия Нерчинская



Александр Панов
VERBA LEGAL



Роман Головацкий
DENUO

Тренды, особенности структурирования и знаковые сделки 2025

2025 г. внес коррективы во взгляды многих игроков на стратегию развития технологических активов. Динамика макропоказателей и текущая конъюнктура рынка сместили переговорный баланс в сторону покупателя, что предопределило изменение логики транзакционного процесса. Отбор новых инвестиционных проектов стал более адресным и сфокусированным, отношение к риску — более осторожным, требования к качеству активов — более строгими.

Значимой особенностью анализируемого периода, отмеченной большинством экспертов, стало усложнение структурирования сделок. Многие инвестиционные проекты в сегменте tech совершались в несколько этапов, в рамках одного этапа в капитал могли войти инвесторы разного профиля (например, финансовые и стратегические), в структурах сделок преобладали комбинации cash-in и cash-out, а финансовые игроки нередко выступали в формате синдиката. Это потребовало выстраивания более гибкой системы отношений между всеми участниками сделки и балансировки их интересов.

Финансовым инвесторам нередко приходилось адаптироваться к ситуации входа стратегического игрока и переформатированию бизнеса в СП с лидирующей позицией стратега. Технологические компании помимо финансовых ресурсов все чаще нуждались в различных нефинансовых компетенциях и рассматривали партнерство с игроками, которые могли усилить их клиентскую базу, обеспечить дополнительные каналы дистрибуции и источники выручки. Новые экономические реалии потребовали от финансовых инвесторов не только фокусировки на контроле за предоставленным финансированием, динамике стоимости своей доли и возврате вложений с доходностью, но и более активного участия в операционных процессах и поиске возможностей для развития бизнеса.

В 2025 г. рынок Tech M&A перешел к более зрелой и прагматичной модели. Отбор проектов стал более строгим и сфокусированным, а инвестиционные тезисы сделок чаще основывались на конкретных прикладных эффектах — измеримых синергиях, подтвержденных финансовых результатах, закрытии продуктовых или технологических пробелов, усилении вертикалей.

Процессы консолидации ранее приобретенных активов в 2025 г. несколько замедлились. Это обусловлено пересмотром инвестиционных приоритетов и подходов к оценке эффективности текущих проектов. В 2025 г. на рынке частного капитала в сегменте tech наблюдалось и движение в сторону деконсолидации. Стратегические инвесторы стремились привлечь партнера в текущие проекты и нередко частично выходили из ранее приобретенных активов для продолжения развития бизнеса в формате СП. Необходимость разделения рисков сформировала в 2025 г. тренд на переход к модели СП в его различных вариациях, в том числе выходящих за пределы классических паритетных структур.

Передача контроля стратегическому инвестору и реализация выхода остальных участников проекта стали более растянутыми во времени. В условиях неопределенности стратегические инвесторы стремились обеспечить более широкие возможности сохранения status quo, включая продолжительные earn-out периоды и сроки реализации опционов-колл, а в ряде случаев — право выхода из актива посредством реализации опциона-пут.

Эти особенности периода сделали качество юридического структурирования одним из главных факторов успешности сделок Tech M&A и их эффективной реализации.

#ТРЕНДЫ



Артур Шубаев

партнер и исполнительный директор инвестиционного банка

ADVANCE CAPITAL

2025 г. стал для российского рынка Tech M&A периодом перехода к более зрелой и избирательной модели сделок с фокусом на стратегические сделки. На фоне высокой ключевой ставки и более осторожного отношения к риску участники стали значительно требовательнее к качеству инвестиционных кейсов. Если в предыдущие периоды значительная часть интереса могла строиться вокруг темпов роста, перспективной ниши или общего тезиса импортозамещения, то в 2025 г. в центре внимания оказались подтвержденные финансовые показатели, качество продукта, устойчивость клиентской базы и наличие понятных синергий для покупателя.

При этом в секторе происходил ряд знаковых крупных транзакций, включая сделки с Аквариусом, Selectel и Avito. Однако, в отличие от предыдущих периодов, крупные сделки стали носить более точечный и стратегически выверенный характер: покупатели были готовы рассматривать значимые инвестиции преимущественно в случаях, когда актив позволял усилить существующий продуктовый, инфраструктурный или клиентский контур.

Для стратегических инвесторов значение приобрели способность актива закрывать конкретный продуктовый пробел, усиливать технологический стек, расширять клиентский доступ или ускорять развитие собственной платформы. В этом смысле показательными являются сделки Яндекса по приобретению Boxberry и Академ-Онлайн: в обоих случаях логика сделки выходила за рамки классического финансового инвестирования и была связана с усилением конкретных направлений экосистемы — логистической инфраструктуры и B2B TravelTech направления соответственно.

Еще одна важная особенность 2025 г. — это повышение роли mid-market сегмента. Именно в среднем сегменте продолжали формироваться новые практики структурирования, взаимодействия между продавцами и покупателями. Такие сделки часто сложнее с операционной точки зрения: компании уже обладают значимым про-

дуктом и клиентской базой, но при этом могут не иметь полностью «институционального» уровня подготовки. Это требует от консультантов более комплексного подхода и более тесной координации между различными департаментами бизнеса и инвесторами.

В целом рынок Tech M&A в 2025 г. стал более качественным. Участники сделок стали тщательнее смотреть на то, как именно будет реализована стоимость после закрытия: кто останется в команде, как будет проходить интеграция, какие риски могут ограничить использование продукта, насколько реалистичны синергии и какие механизмы позволяют закрепить договоренности сторон. Это делает сделки более сложными, но одновременно повышает их устойчивость и качество инвестиционных решений.

> **В 2025 г. в условиях высокой стоимости капитала, снижения риск-аппетитов покупателей и низких мультипликаторов оценки качество и гибкость юридического структурирования стали одним из ключевых факторов успешности сделок Tech M&A.**

#ТРЕНДЫ



Юлия Загорнова

партнер Группы компаний Б1

Оценив ландшафт сделок в 2025 г., можно сказать, что несмотря на высокую стоимость денег, ИТ все еще остается достаточно универсальной отраслью с точки зрения интереса инвестора, что можно объяснить как растущим проникновением ИТ-продуктов во все сегменты экономики, так и ожиданием инвесторов, что именно в ИТ сегменте все же кроется наиболее «близкий» источник роста. В нашей практике мы отмечаем растущий интерес к технологическим компаниями даже со стороны инвесторов, которые никогда не были связаны с ИТ и до сих пор инвестировали исключительно в производственные индустрии. При этом подход к отбору проектов стал намного более строгий и детальный. Все это не могло не отразиться как на времени, необходимом для закрытия сделки, так и на закрываемости сделок в целом.

Основной проблемой в прошлом году, безусловно, стала высокая стоимость денег, что существенно повлияло на ценовые ожидания и аппетит к риску со стороны покупателей и заставило задуматься продавцов активов, не перегруженных внешним долгом, о том, правильный ли сейчас момент для продажи. На фоне этого многие инвесторы стали отмечать нехватку качественных активов для инвестиций и слишком высокие ожидания по оценке со стороны тех продавцов, кто все же решился попробовать продать бизнес, что требовало большей гибкости в переговорах и, как итог, более многоступенчатого структурирования сделок.

Также, помимо более креативного подхода к ценообразованию и структурированию сделок, мы можем отметить возросший запрос со стороны стратегических инвесторов на сохранение основателя приобретаемого бизнеса в компании в качестве миноритарного акционера в долгосрочной перспективе, чтобы бизнес оставался более операционно стабильным, команда была спокойна, а рынок продолжал видеть в компании надежного партнера, не подверженного рыночной турбулентности.

В целом по сравнению со многими другими индустриями рынок сделок с технологическими компаниями оставался в 2025 г. достаточно живым и активным, запрос инвесторов на приобретения и инвестиции в компании не снижался, однако повысилась сложность процесса и сместились акценты в переговорах.

#ТРЕНДЫ



Роман Головацкий

партнер

DÉNUO

@DENUOLAW →

Наиболее точно состояние инновационного ландшафта в 2025 г. описано в 18-м выпуске Глобального инновационного индекса Всемирной организации интеллектуальной собственности (World Intellectual Property Organization (WIPO) (2024). Global Innovation Index 2025: Innovation at a Crossroads. Geneva: WIPO. DOI: 10.34667/tind.58864). Документ, в частности, отмечает, что мир вновь стоит на пороге глобального перехода: технологические прорывы сменяют друг друга с беспрецедентной скоростью, а развитие искусственного интеллекта, от базовых моделей до автономных систем, обещает существенно изменить промышленность, рынки труда и социальные структуры.

В этой связи сектор информационных технологий продолжает оставаться одним из ключевых драйверов крупных сделок и концентрации капитала в мире. Российская Федерация не является исключением: сделочная активность в сфере ИТ сохраняет интенсивность, несмотря на тектонические экономические сдвиги. Рынок по-прежнему демонстрирует стремление к консолидации активов вокруг крупных игроков бигтеха.

Вместе с тем не теряет актуальности сформировавшийся за последние годы запрос на декомпозицию ИТ-продуктов для внутреннего и внешнего рынков в рамках M&A-сделок, с тем чтобы продавцы сохраняли возможность развивать международное направление и обеспечивать самостоятельную эволюцию своего продукта отдельно от продукта покупателя.

Эти особенности сопровождаемых нами сделок требовали поиска нестандартных юридических решений как в сфере интеллектуальной собственности, так и в корпоративном праве, чтобы выработать оптимальную структуру и корректно «расщепить» права на нематериальные активы. В таких условиях особенно важно соблюсти баланс интересов сторон и предусмотреть механизмы, которые позволят не только защитить права приобретателя, но и сохранить коммерческую ценность выделенного продукта для продавца и потенциал его дальнейшего развития на международных рынках.

Мы попросили лидеров M&A-практик ведущих юридических консультантов рассказать о наиболее знаковых сделках Tech M&A 2025 г. и особенностях их структурирования, а также отметить актуальные тренды юридического сопровождения сложных технологических проектов, которые они наблюдали в своей практике на протяжении прошедшего года.

#ОСОБЕННОСТИ_СТРУКТУРИРОВАНИЯ



Сергей Крохалев

партнер практики корпоративного права / слияний и поглощений

Melling Voitishkin &Partners

В 2025 г. на рынке Tech M&A можно было выделить несколько трендов, которые проявились в ряде знаковых проектов:

1. **Создание совместных предприятий (СП) между стратегическими инвесторами и технологическими компаниями**. Нередко — с возможностью на согласованном горизонте полного выкупа партнера стратегическим инвестором. В качестве примера можно привести проект по созданию СП между Yandex B2B Tech и SolidSoft, разработчиком Web Application Firewall. Ключевой сложностью в таких сделках является структурирование вопросов интеллектуальной собственности: как разделить права на уже существующие технологии и на те, что будут созданы совместно. На первый план также выходит задача по разработке сбалансированной мо-

дели корпоративного управления, которая защитит инвестиции стратегического партнера, но при этом сохранит гибкость и экспертизу команды основателей технологической компании.

2. **Сделки с участием топ-менеджмента (MBO)**. Показательным был проект по приобретению инвесткомпанией контроля в российской финтех-компании, где топ-менеджмент также выступил покупателем миноритарной доли. Главный вызов здесь — правильное выстраивание системы сдержек и противовесов между финансовым инвестором и управляющей командой. Актуальным риском является потенциальный конфликт интересов. Поэтому особое внимание уделялось разработке корпоративного договора, учитывающего данную структуру собственности, и одновременно — созданию системы мотивации ключевых членов команды, чтобы синхронизировать долгосрочные цели всех сторон и мотивировать менеджмент на достижение согласованных КПЭ.
3. **Реструктуризация и продажа российского бизнеса международными компаниями**. Мы помогли клиенту с реализацией сложного проекта по выходу международного телеком-оператора с российского рынка. Особенностью таких сделок является их двухэтапность: сначала — юридически и технически сложный процесс выделения локального бизнеса из глобальной структуры (carve-out), а затем — его продажа. Основной проблемой в 2025 г. оставалось прохождение регуляторных процедур, в частности получение согласований от ФАС и Правительственной комиссии, что на практике может создавать серьезную неопределенность в сроках закрытия сделки. Это требует учета данного фактора как при подготовке документов по сделке, так и в операционных аспектах деятельности таргета. На первый план также выходили вопросы разделения ИТ-систем, трансграничного лицензирования ИС и переоформления коммерческих контрактов.

4. **Сделки на рынке медиа и контента (OTT-сервисы)**. При продаже одного из крупных российских аудиовизуальных OTT-сервисов проявилась нетипичная для классических M&A проблематика. Важным вызовом стал технически и юридически сложный процесс миграции огромной пользовательской базы к покупателю и нахождение правильной мотивации сторон для того, чтобы сохранять вовлеченность на протяжении всего процесса миграции (в такого рода проектах это может быть период в 1–1,5 года). Поскольку этот бизнес находится под пристальным вниманием регуляторов, распределение рисков между продавцами и покупателями в рамках документов по сделке не было простым.

#МНЕНИЕ_ЛИДЕРОВ_РЫНКА

На гребне технологического бума



Леонид Эрвиц
управляющий партнер, глава корпоративной практики

2025 г. подтвердил статус технологического сектора как одного из ключевых драйверов российского рынка M&A. На фоне структурной трансформации экономики мы наблюдаем устойчивый рост сделочной активности в данном секторе, обусловленный, с одной стороны, продолжающейся консолидацией активов вокруг крупнейших цифровых экосистем, а с другой, — повышенным интересом стратегических инвесторов к нишевым и высокоспециализированным технологическим решениям. В фокусе большинства транзакций находятся задачи расширения и диверсификации продуктовых линеек, усиления технологической экспертизы и достижения синергетического эффекта за счет интеграции уникальных цифровых платформ, сервисов и команд разработки.

Рынок в большей степени ориентирован на задачи обеспечения технологической независимости и импортозамещения, а игроки — на укрепление позиций в сегментах B2B-IT и высокоспециализированных цифровых решений. Такие транзакции, как правило, отличаются повышенной структурной и регуляторной сложностью, что обуславливает необходимость глубокого правового сопровождения на этапах оценки активов, структурирования сделок и управления юридическими рисками. За последнее время команда LEVEL Legal Services сопровождала ряд знаковых транзакций, определяющих ландшафт рынка, из которых можно выделить следующие:

(1) Продажа сервиса «Бери Заряд!» группе Яндекс

Сделка по продаже бизнеса АО «Заряд» (лидер рынка шеринга пауэрбанков) в пользу Группы «Яндекс» стала важным этапом развития сегмента экономики совместного потребления («sharing economy»). Сделка была осложнена выкупом акций у более чем 200 акционеров-миноритариев, инвестировавших в компанию в рамках pre-IPO раунда. Также в рамках сделки был использован такой нестандартный инструмент, как условное депонирование акций с множественностью сторон. Интеграция компании в экосистему Яндекс открывает новые перспективы для ее дальнейшего развития.

(2) Приобретение Яндекс Путешествиями платформы «Академ-Онлайн»

Сделка по приобретению цифровой платформы «Академ-Онлайн» была реализована в рамках развития Яндекс Путешествиями направления делового туризма. Как и в других сделках, связанных с приобретением и последующей интеграцией в существующую цифровую экосистему технологических компаний, основным активом которых являются объекты интеллектуальной собственности, ключевой фокус уделялся оценке прав на такие объекты. Существенное значение имеет проверка прав на программное обеспечение, базы данных и иные нематериальные активы, а также выявление потенциальных рисков, способных повлиять на дальнейшее использование актива и их учет при структурировании сделки.

(3) Инвестирование Группы Arenadata в разработчика MDM-решений

Сделка по привлечению стратегического инвестора с долей участия 20% в уставном капитале разработчика MDM-решений была ре-

ализована в целях развития разработчиком бизнеса в сфере управления данными и расширения продуктовой линейки. Проект предполагал формирование долгосрочной партнерской модели с участием инвестора, что повлекло необходимость детальной проработки параметров партнерства и выстраивания баланса интересов сторон. В подобных сделках существенное внимание уделяется структуре корпоративного управления, распределению контроля и механизмам принятия решений, а также порядку финансирования проекта сторонами. Важной частью структурирования условий сотрудничества также является определение случаев и способов выхода из инвестиции, детальная проработка которых на старте позволяет снизить риски корпоративного конфликта (и его тяжести) в будущем.

#ТРЕНДЫ



Арташес Оганов

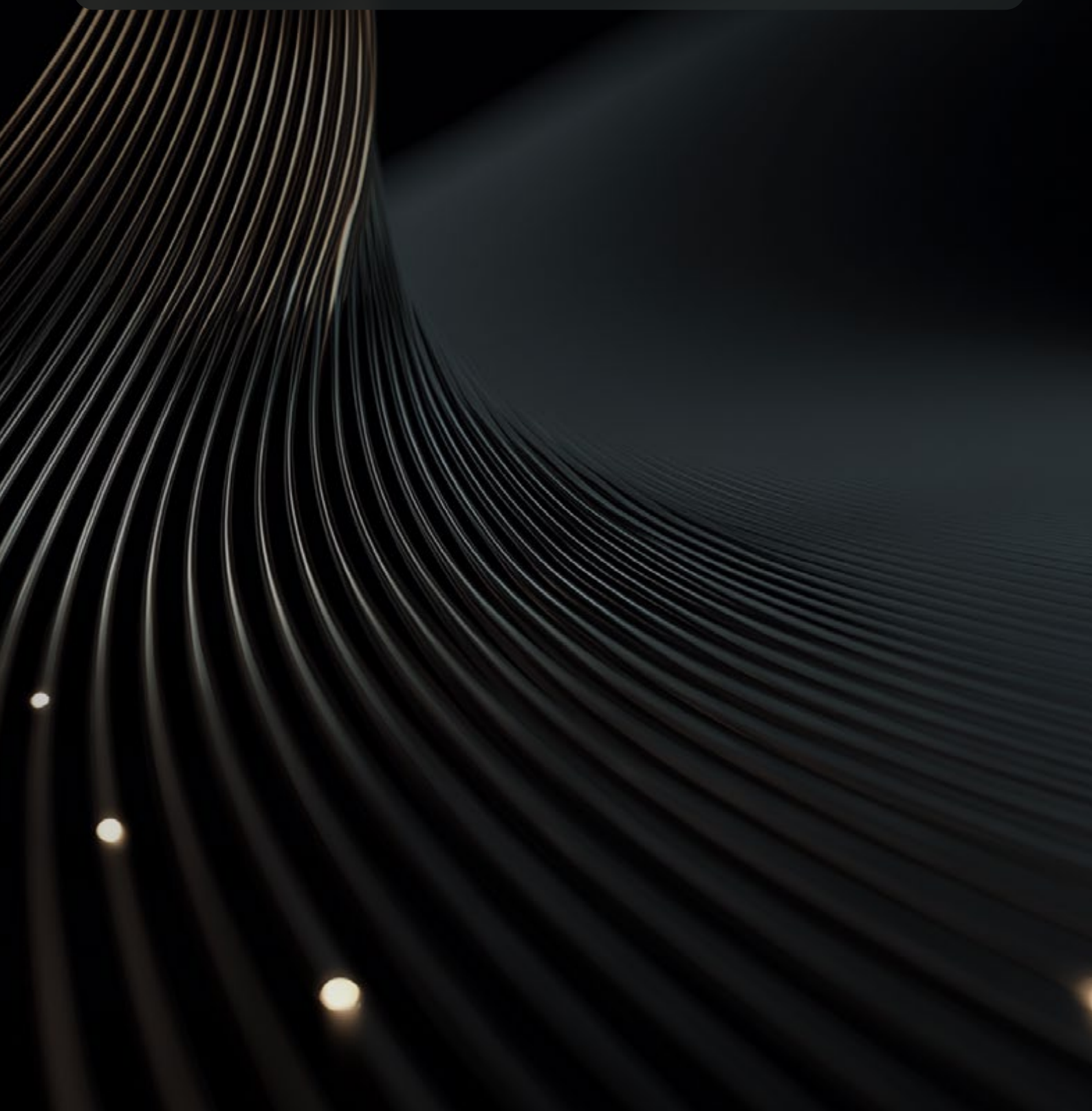
партнер, глава практики корпоративного права / M&A

sll
SL LEGAL

В текущих экономических реалиях сегмент Tech M&A остается одним из немногих «живых». Здесь по-прежнему регулярно происходят сделки, и важно, что подавляющее большинство этих сделок — рыночные. Но, конечно, общий тренд на спад экономической активности повлиял и на Tech M&A. Основываясь на опыте сделок, которые проходят через нашу фирму, можно выделить ряд общих черт, которые характерны для текущих проектов в этом секторе.

1. Большинство сделок происходит в бизнесах, которые прошли этап первоначального роста и уже могут продемонстрировать успешные операционные показатели. То есть инвесторы все больше отказываются от «лотереи» с венчурными инвестициями на ранних этапах развития компании. В условиях ограниченной ликвидности и высокой ключевой ставки аппетит вызывают уже проверенные временем бизнесы с понятными перспективами, которые с большей вероятностью продолжат масштабироваться и обеспечат доходность, превышающую ставки по банковским депозитам.
2. Со стороны инвесторов наибольшую активность проявляют крупные игроки — структуры госкомпаний, частные многопрофильные холдинги, банковские группы и лидеры IT-индустрии. Присматриваясь к новому активу, потенциальные покупатели больше рассчитывают на его интеграцию в свой существующий бизнес и возможную синергию, чем на дальнейшее развитие в качестве независимого игрока.
3. Практически во всех случаях одним из требований покупателя является сохранение основателя в управленческой роли. Даже при покупке мажоритарной (а иногда и 100%-ой) доли инвестор настаивает, чтобы основатель продолжал управлять операционной деятельностью и развивать бизнес. Покупатели готовы предоставлять основателю достаточно широкую самостоятельность в принятии управленческих решений. Это еще один способ для инвестора обеспечить успешную траекторию развития актива и снизить риск неудачной инвестиции.

Чтобы сохранить финансовую мотивацию для основателя, подавляющее большинство сделок предусматривает использование механизма earn-out при расчете покупной цены: итоговая сумма вознаграждения за продаваемый актив определится только по итогам его деятельности через 1–3 года после покупки.



#МНЕНИЕ_ЛИДЕРОВ_РЫНКА

Предпродажная реструктуризация: консолидация IT и IP активов в приобретаемом контуре до закрытия сделки и механизмы договорной защиты покупателя



Максим Кулешов
управляющий партнер

KKMP LEGAL

Наша команда консультировала покупателя в сделке по приобретению бизнеса, операционная деятельность которого в существенной степени зависела от собственной программной инфраструктуры. В активах таргета было более 40 специализированных программ, задействованных в ключевых бизнес-процессах, в том числе для взаимодействия холдинга и оптовых партнеров, управления циклом производства и реализации изделий. Программное обеспечение разрабатывалось как внутренними командами, так и многочисленными внешними подрядчиками, что усложняло проверку титула.

Дополнительную специфику бизнесу придавало его историческое разделение на два контура: основной, принадлежащий иностранному юридическому лицу, и дополнительный, состоящий из нескольких компаний, принадлежащих физическим лицам, аффилированным с продавцом.

Такая структура обусловила удлинение сроков юридической проверки, в ходе которой был выявлен ряд рисков и особенностей, повлиявших на дальнейшее структурирование сделки, а именно: (1) риски отсутствия исключительных прав компаний группы на ключевое программное обеспечение, (2) принадлежность основных объектов интеллектуальной собственности разным лицам за пределами периметра группы в нескольких юрисдикциях, и (3) наличие в приобретаемом контуре части активов бенефициара, не связанных с деятельностью таргета.

Выявленные риски и особенности актива обусловили следующие действия по митигации и предпродажной реструктуризации:

(1) Оформление прав на ПО

Было заключено порядка 100 соглашений с разработчиками для надлежащего оформления прав приобретаемой группы на разработанное программное обеспечение.

(2) Реструктуризация

Владение компаниями дополнительного контура было передано от физических лиц в пользу холдинговых компаний.

(3) Консолидация портфеля интеллектуальной собственности

в периметре сделки, которая имела следующие особенности:

- Поскольку объекты интеллектуальной собственности были зарегистрированы в нескольких юрисдикциях и принадлежали различным компаниям группы, их консолидация в периметре сделки потребовала отдельной регистрации перехода прав по национальным и международным процедурам.

- В ряде случаев продавцом была осуществлена регистрация перехода прав по заявлению сторон без заключения договора об отчуждении исключительных прав и выплаты вознаграждения, что создавало риск оспаривания. Для устранения налоговых рисков и снижения вероятности оспаривания сделок потребовалось заключить ряд возмездных договоров по рыночной стоимости.
- Передача портфеля интеллектуальной собственности покупателю предполагала запрет на использование сходных обозначений продавцом, что повлекло изменение фирменных наименований компаний продавца и прекращение использования продавцом сходных доменных имен.

(4) Вывод активов продавца из периметра сделки

в пользу лиц из группы продавца был осложнен трудностями с проведением расчетов, в связи с чем был реализован механизм уступки прав требования и зачета против части покупной цены в рамках основного ДКП.

Особенностью данной сделки являлось то, что предпродажная реструктуризация проводилась продавцом до заключения какой-либо обязывающей документации параллельно с ведением переговоров. Со стороны покупателя корректность всех действий проверялась сразу же в рамках подтверждающей юридической проверки. В той части, в которой реструктуризация не была завершена до закрытия, соответствующие действия перешли в обязательства группы продавца после закрытия, закрепленные в ДКП.

Помимо этого, ДКП (подчиненный гонконгскому праву) содержал ряд защит покупателя для минимизации рисков проведенной реструктуризации:

- Отдельное приложение, конкретизирующее все реализованные шаги.
- Обязательства по возмещению имущественных потерь покупателя: общее обязательство на случай, если какие-либо действия в рамках реструктуризации не были совершены или совершены ненадлежащим образом, обязательство о возмещении потерь в отношении налогов для покрытия всех совершенных действий и заключенных сделок, а также в отношении утраты или обременения титула на объекты интеллектуальной собственности.
- Обязательства продавца обеспечить, чтобы лица из группы продавца не создавали, не регистрировали и не использовали после закрытия какие-либо аналогичные объекты интеллектуальной собственности.
- Широкие заверения продавца в отношении действительности и надлежащего заключения всех необходимых соглашений, а также отдельное заверение в отношении того, что все объекты интеллектуальной собственности, необходимые для осуществления деятельности таргета, были переданы в периметр сделки. Стоит отметить, что ключевые заверения о правоспособности и титуле также были включены в соглашения с аффилированными лицами продавца, заключенные в рамках реструктуризации.

#ОСОБЕННОСТИ_СТРУКТУРИРОВАНИЯ



Евгений Юрьев

партнер

NIKOLSKAYA consulting

Одной из сделок в сфере TMT, в которые мы были вовлечены в этом году, было приобретение крупным игроком на TMT рынке одного из лидеров российского рынка по разработке ПО в сфере связи. Особенностью данной сделки являлось то, что, несмотря на приобретение формального корпоративного контроля у основателей, последние сохранили широкую самостоятельность в операционном управлении группой.

Структурирование сделки осложнялось тем, что, несмотря на достижение сторонами коммерческой договоренности по распределению полномочий между покупателем и основателями, такие договоренности не могли быть прямо воплощены в документах по сделке из-за требований консолидации таргета в группе покупателя. В связи с этим нашей команде пришлось искать нестандартные решения, которые позволили бы воплотить коммерческие договоренности сторон без нарушения правил о консолидации. Так, например, часть согласованных механизмов управления была реализована через набор триггеров для дефолтных опционов вместо обязательств по корпоративному договору, другая часть была реализована через специальные механизмы, которые, не затрагивая правил о кворуме или большинстве для принятия решений (которые покупатель должен был иметь право принять самостоятельно), позволили обеспечить негативный контроль основателей за принятием решений по согласованным вопросам.

Другой особенностью сделки стала необходимость распределения ответственности за риски, связанные с ПО, в случае их реализации на промежутке, когда основатели уже выйдут из компании. Классические ограничения ответственности продавца предполагают полный контроль продавца над процессом рассмотрения требований третьих лиц, однако такой подход может быть не оптимальным при реализации рисков на средней и дальней дистанции, так как после окончательного выхода основатели могут быть не заинтересованы в урегулировании требований в выгодном для компа-

нии формате. В результате нам удалось достичь создания компромиссного механизма, который бы обеспечивал контроль основателей за удовлетворением таких требований, пока они принимают участие в деятельности компании, и вступление в силу квазифидуциарного механизма рассмотрения таких требований покупателем после их окончательного выхода.

#ОСОБЕННОСТИ_СТРУКТУРИРОВАНИЯ



Александр Венгранович

управляющий директор,
начальник управления слияний
и поглощений

СОВКОМБАНК

В 2025 г. мы сопровождали ряд сделок по приобретению и продаже Tech-бизнесов, в том числе в форматах minority / majority. Сделки реализовывались как на стороне покупателя / инвестора, так и на стороне продавца.

Ключевой особенностью юридического сопровождения сделок Tech M&A в 2025 г. стало существенное усложнение структуры сделок и усиление фокуса на управляемости рисков после закрытия. Во многих случаях стандартные SPA-структуры дополнялись отложенными платежами, earn-out, escrow и иными механизмами перераспределения рисков между сторонами.

Со стороны покупателя приоритетное внимание уделялось проверке прав на интеллектуальную собственность (цепочка прав, корректность IP-assignment, риски open source), вопросам информационной безопасности и обработки данных, а также регуляторному статусу бизнеса.

Существенную роль играла проверка корпоративной структуры, ограничений на отчуждение долей / акций и потенциальных рисков, связанных с санкционным контуром и иностранным элементом.

В сделках в сегментах FinTech, AI / ML, кибербезопасности и B2B Software ключевыми юридическими особенностями являлись вопросы надзорных требований, соблюдение законодательства о персональных

данных и критической информационной инфраструктуре, а также повышенные требования к документированию технологических решений и алгоритмов. В ряде случаев именно регуляторные и ИБ-аспекты оказывали определяющее влияние на структуру сделки и сроки ее закрытия.

В целом следует отметить, что в 2025 г. юридическая функция в Tech M&A все чаще выходила за рамки «поддерживающей» роли и трансформировалась в элемент сделки, влияющий как на цену, так и на исполнимость договоренностей.

#ТРЕНДЫ



Константин Олефир

партнер

ORION

К наиболее значимым аспектам сделок Tech M&A в 2025 г., по моим наблюдениям, можно отнести следующие:

1. Ограниченный пул стратегических инвесторов на рынке и полярность в подходах к приобретению компаний: покупка 100% долей или многостадийное приобретение (миноритарная доля + опционы на приобретение контроля).
2. Необходимость учитывать, совершал ли таргет pre-IPO-размещения при планировании сделки, так как могут возникать сложности с выкупом акций частных розничных инвесторов.
3. В ряде случаев интеграция таргета в бизнес-вертикали подсанкционного приобретателя может осуществляться в теневом режиме.
4. Большое внимание уделяется сохранению мотивации менеджмента по развитию бизнеса компании после ее приобретения.

Аспекты в фокусе внимания

Сделки в сегменте tech в силу отраслевой специфики всегда отличались не только сложностью оценки, но и комплексным юридическим структурированием, требующим особой гибкости в использовании транзакционных инструментов и поиска нестандартных решений. В ходе исследования мы попросили ведущих игроков рынка, участвующих в сделках Tech M&A в 2025 г., рассказать о юридических аспектах, на которых команды продавца и покупателя бизнеса фокусировались в первую очередь, и какие вопросы требовали особого внимания.

#ФОКУС_ВНИМАНИЯ



Вячеслав Поджаров

старший менеджер проектов инвестиционного банка

ADVANCE CAPITAL

Команда продавца в большей степени была сфокусирована на подготовке периметра сделки и корректном расчете финансовых показателей. На практике это означало необходимость заранее проверить и, при необходимости, дооформить права на ПО, урегулировать отношения с разработчиками, подтвердить корректность применения налоговых льгот, подготовить договорную базу с ключевыми клиентами и описать технологическую архитектуру продукта. Чем лучше продавец подготовлен к этим вопросам, тем меньше вероятность, что due diligence приведет к существенным пересмотрам ценового предложения, дополнительным отлагательным условиям или удержанию части цены.

Отдельное внимание обе стороны уделяли механике распределения рисков в документации. Для покупателя это означало расширенные заверения и indemnity, отложенные платежи на ИТ-составляющую. Для продавца это означало сокращенные лимиты ответственности, прозрачные правила расчета earn-out, ограничение периода предъявления требований и защиту от субъективного влияния покупателя на будущие KPI.

#МНЕНИЕ_ЛИДЕРОВ_РЫНКА

Tech M&A: адаптация классических правил игры



Булат Жамбалнимбуев
партнер и руководитель
корпоративной практики

NEXTONS

Ключевой фокус при согласовании сделки Tech M&A направлен на получение контроля над технологией, командой и будущей экономикой продукта. В этом смысле сделка с технологическим активом — это больше не классическая дихотомия выбора между share и asset-deal, а индивидуальное выстраивание структуры сделки с акцентом на формирование долгосрочной управляемости актива и конструирование контроля над тем, где создается ценность. На смену универсальным M&A решениям пришло ситуационное структурирование, где финальная юридическая конструкция — не формальное отражение договоренностей сторон, а реальный инструмент управления инвестиционными рисками.

На практике это означает, что:

1. Покупатель проводит глубокие предынвестиционные проверочные мероприятия актива.
2. Формальному закрытию сделки (а зачастую и подписанию транзакционной документации) предшествует многошаговая комплексная реструктуризация, направленная на изоляцию технологического периметра и переупаковку IP- и RD-функций с фокусом на корректную передачу исключительных прав, сохранение непрерывности разработки и минимизацию утечек.
3. В условиях неопределенной оценки и быстро меняющейся технологической среды мы все чаще наблюдали запросы на:

- Поэтапное вхождение в проект (через приобретение миноритарной доли и ее постепенное увеличение) и использование сложных earn-out моделей (привязанных к достижению определенных отдельных продуктовых стадий, готовности технологии к масштабированию и / или успешной интеграции в экосистему инвестора) для валидации технологии, основных рабочих гипотез и команды.
- Использование опционных конструкций как инструмента последующей консолидации при подтверждении инвестиционной гипотезы.
- Изъятие (перенос) ключевых активов из проблемного или избыточно рискованного корпоративного контура через asset-deal.
- Разработку сложных мотивационных и удерживающих механизмов для ключевых членов команды.
- Получение контрактного контроля над технологией (в том числе через лицензионные схемы с элементами эксклюзивности) без необходимости юридической консолидации, обеспечивающее быстрый доступ к IP и команде.

#ФОКУС_ВНИМАНИЯ



Леонид Эрвиц

управляющий партнер, глава корпоративной практики

LEVEL Legal Services

Наш опыт сопровождения Tech M&A сделок на стороне покупателя в 2025 г. показывает, что последний, как правило, в большей степени сосредоточен на таких аспектах, как: (i) создание эффективной договорной модели борьбы с утечками в период между подписанием и закрытием сделки, (ii) грамотный подбор заверений об обстоятельствах, максимально соответствующих конкретной компании и ее бизнес-модели, (iii) «закрытие» максимального числа материальных рисков, выявленных в рамках due diligence с использованием механизма возмещения имущественных потерь, (iv) конструирование комплементарных для покупателя договорных стандартов раскрытия информации, ограничивающих действие заверений об обстоятельствах, и тщательная работа с предоставленным продавцом проектом письма о раскрытии, (v) борьба с желанием продавца ограничить свою ответственность (как по срокам, так и по суммам) — особенно в части титулярных и налоговых рисков, а также несогласованных утечек.

Если одновременно с закрытием сделки или сразу после него планируется поменять управленческую команду таргета, то команда покупателя также может уделять большое значение положениям договора, посвященным эффективному «перехвату» управления компанией после закрытия.

В пределах, в которых это возможно с учетом антимонопольных и иных рисков, некоторые покупатели также проявляют интерес к фиксации условий о неконкуренции основателей с проданным им таргетом, а также о непереманивании ключевых сотрудников таргета в течение определенного срока.

Вопрос цены также немаловажен — многие покупатели стремятся к внедрению в сделку механизмов, позволяющих не выплачивать за таргет все сразу (рассрочка, earn-out, опционные конструкции и т. д.).

#ФОКУС_ВНИМАНИЯ



Анастасия Духина

старший юрист практики корпоративного права / M&A

SLL

В условиях ограниченной ликвидности на рынке и «дорогих» денег приобретатели в большинстве случаев максимально фокусируются на защите своих инвестиций, поэтому особое внимание уделяется ответственности продавца в случае несоответствия компании ожиданиям приобретателя. Так, при частичном вхождении инвестора в компанию тщательно прорабатываются механизмы досрочного выхода инвестора (в большинстве случаев с получением повышенной доходности) или перераспределения контроля (увеличения контроля инвестора и снижения контроля основателя) в случае нарушений со стороны продавца. При приобретении 100% компании также тщательно прорабатываются положения об ответственности продавца и размере компенсации, выплачиваемой покупателю в случае возникновения проблем в компании после сделки (штрафы, возмещение имущественных потерь, заранее оцененные убытки и т. д.), а также покупатель стремится закрепить максимально долгий период, когда продавец может быть привлечен к такой ответственности.

#ФОКУС_ВНИМАНИЯ



Владислав Лазуткин

старший юрист

ORION

В сделках Tech M&A, которые мы сопровождали в 2025 г., команда приобретателя была сфокусирована преимущественно на следующих вопросах:

- Структура и порядок расчетов: модель ценообразования, отложенный платеж.
- Структура выкупа: выкуп 100% или многоэтапное приобретение (в том числе с элементами cash-in).
- Объем ответственности продавцов — мажоритарных и миноритарных акционеров (в том числе финансовых инвесторов).

#ФОКУС_ВНИМАНИЯ



Байрас Магадеев

старший юрист
корпоративной практики

ELWI

В рамках сделки по приобретению онлайн-сервиса по предоставлению медицинских услуг мы осуществляли полное юридическое сопровождение на стороне покупателя. Основной фокус покупателя был направлен на проверку титула таргета в отношении программного обеспечения, мобильных приложений и модулей, используемых таргетом в хозяйственной деятельности, и поэтому рассматривавшихся покупателем как ключевой актив таргета, а также сопутствующих вопросов. Соответственно, значительные усилия коммерческих команд сторон были направлены на согласование вопросов ответственности продавцов в случае обнаружения каких-либо пороков в отношении ключевых активов. В итоге в договоре были предусмотрены стандартные механизмы защиты интересов покупателя, а также максимальный лимит ответственности продавцов по вопросам, связанным с ключевыми активами.

#ФОКУС_ВНИМАНИЯ



Артем Тамаев

партнер корпоративной
практики и M&A

BETTER CHANCE

Мы отмечаем существенный рост актуальности вопросов неконкуренции в ИТ сфере. При формировании совместных предприятий стороны очень детально подходят к договорному разграничению разрешенных и запрещенных сфер для дальнейшего развития и инвестирования. Такие инструменты часто подлежат согласованию с антимонопольным регулятором, что нередко усложняет и удлиняет общий таймлайн сделки.

Раздел 2

Структуры и форматы сделок Tech M&A в 2025 г.

АВТОРЫ



Анастасия Нерчинская



Александр Панов
VERBA LEGAL



Роман Головацкий
DENUO

Краткие выводы

- В 2025 г. сделки синдицированного cash-in инвестирования были наиболее распространенным инвестиционным форматом. При этом доля «классических» сделок cash-in с участием нескольких инвесторов была существенно выше числа проектов формата pre-IPO с широким кругом участников, совершаемых с использованием инвестиционных платформ.

- Для большинства технологических компаний, особенно продуктовых, не имеющих hardware-составляющей, equity-инвестиции являются основным доступным источником финансирования. По причине отсутствия залоговой массы возможности привлечения кредитов для таких компаний сильно ограничены. Этим объясняется широкое распространение элемента cash-in в сделках Tech M&A любого формата. В 2025 г. эта тенденция усилилась в связи с дефицитом текущей ликвидности многих IT-компаний.

- В 2025 г. существенная доля Tech M&A-проектов сочетала элементы cash-in и cash-out. Инвесторы, помимо предоставления инвестиций компании, также частично выкупали доли основателей бизнеса или инвесторов предыдущих раундов. Многие из таких сделок совершались с участием стратегических приобретателей, которые выкупали часть доли основателей бизнеса, обеспечивая им возможность реализации частичного выхода из проекта и фиксации созданной стоимости.

- В 2025 г. наиболее популярным форматом участия в технологических компаниях стало приобретение пакета «существенного влияния» в размере от 35% до 49%. Это обусловлено множеством факторов, основным из которых является изменение инвестиционных стратегий многих крупных игроков (особенно стратегических инвесторов) в сторону более адресных приобретений по результатам тщательной проверки гипотез.

- В 2025 г. на рынке Tech M&A закрепился тренд на формирование СП с преобладанием их «неклассического» формата, не предполагающего обязательного паритетного участия партнеров. Ведущим партнером в таких структурах чаще всего становился стратегический инвестор, который рассматривался как потенциальный консолидирующий участник, способный в будущем выкупить доли текущих инвесторов и основателя.

В ходе исследования мы попросили участников онлайн-опроса отметить, какие структуры сделок с технологическими активами, по их мнению, были наиболее распространены в 2025 г.

#РЕЗУЛЬТАТЫ_ОПРОСОВ

Какие структуры сделок вы чаще использовали, приобретая российские ИТ-компании в 2025 г.?



По данным Опроса по структурированию сделок Tech M&A в 2025 г. (125 респондентов).

Как показали результаты опроса, в 2025 г. сделки с участием синдиката equity-инвесторов были наиболее распространенной моделью инвестирования (отметили **81% респондентов**). Синдицированное финансирование направлено как на закрытие потребностей компаний в текущей ликвидности и оптимизации их долговой нагрузки, так и на масштабирование бизнеса и рост его стоимости. Такой формат инвестиций позволяет расширить продуктовый контур бизнеса, увеличить капитализацию компании, обеспечить ее подготовку к IPO или продаже стратегу и в то же время распределить риски с другими участниками проекта.

Отмеченное многими экспертами увеличение в 2025 г. доли сделок с элементом cash-in обусловлено рядом факторов. В условиях сохраняющейся высокой стоимости финансирования и сжатия корпоративного спроса крупных IT-компаний на продукты внешних вендоров многие развивающиеся бизнесы сегмента tech испытывали нехватку оборотных средств. Проекты с более устойчивым финансовым положением нуждались в инвестициях на расширение бизнеса, включая развитие новых направлений и усиление компетенций. При этом многие технологические компании были заинтересованы в привлечении нефинансовых ресурсов инвесторов, в первую очередь маркетинговых компетенций, новых возможностей контрактации и каналов дистрибуции.

Распространенность синдицированного формата сделок cash-in отметили **81% респондентов**, а сделок, совершаемых по модели «pre-IPO», — только **18%**, хотя на первый взгляд структура и экономика проектов схожи. Такое различие в ответах объясняется тем, что опрос предполагал разделение **всего объема непубличных сделок cash-in на два формата**: (i) классический вариант equity-инвестиций с участием 2–3 финансовых инвесторов, предоставляемых компании за 1–2 года до выхода на биржу, и (ii) сделки pre-IPO в узком понимании этого термина, предполагающие привлечение денежных средств в капитал компании от широкого круга инвесторов с использованием инвестиционных платформ — MOEX Start, ВТБ Регистратор и других. В 2025 г. сделок первого — классического формата cash-in, — было значительно больше, чем сделок второго типа, что и было отражено в итогах опроса.



Александр Кузнецов

партнер, руководитель практики «Рынки капитала»

VERBA LEGAL

> В последние годы термин «pre-IPO» стал использоваться в маркетинговых целях для сделок по привлечению денежных средств в капитал компании от широкого круга инвесторов с использованием инвестиционных платформ (таких как MOEX Start, ВТБ Регистратор, Zorko, Rounds и т. п.). Таких сделок значительно меньше, чем классических cash-in сделок с участием институциональных инвесторов, совершаемых без использования инвестиционных платформ.

В 2025 г. в структуре сделок Tech M&A наряду с форматом cash-in **существенную долю занимал элемент cash-out**, в том числе **в сочетании с equity-финансированием**. Это свидетельствует о том, что помимо предоставления инвестиций компании новые инвесторы также выкупали доли основателей бизнеса (отметили **76% респондентов**) или инвесторов предыдущих раундов (**43% респондентов**), которые реализовывали полный или частичный выход из проекта. Многие из таких сделок **совершались с участием стратегических инвесторов**, которые выкупали часть доли основателя бизнеса. Это позволяло владельцу компании зафиксировать текущую позицию и являлось стимулом для дальнейшего развития актива. В 2025 г. сделки инвестирования с элементом cash-out совершались как в рамках первичного входа стратегического инвестора в капитал, так и при реализации колл-опциона на следующей стадии сделки, направленной на консолидацию участия.

Большинство экспертов, опрошенных нами в рамках исследования, также отметили в 2025 г. высокую активность стратегических инвесторов в сделках Tech M&A. Во многих случаях такие проекты структурировались по модели earn-out с сохранением участия основателя бизнеса как минимум в размере миноритарного пакета.



Артур Шубаев

партнер и исполнительный директор

ADVANCE CAPITAL

Сделки все чаще строились не как простая покупка долей, а как гибкая инвестиционная конструкция, сочетающая докапитализацию бизнеса, частичный cash-out для основателей. Высокая доля cash-in структур с участием синдиката новых инвесторов показывает, что в условиях высокой стоимости капитала и повышенной неопределенности участники рынка стремились разделять инвестиционную нагрузку и одновременно усиливать проект за счет привлечения нескольких партнеров с разными компетенциями.

Особенно хочется выделить значительный объем сделок, который мы видим на своей практике в формате cash-in в сочетании с существенным cash-out фаундеров. Для зрелых ИТ-компаний это естественный этап развития: основатели получают возможность частично зафиксировать созданную стоимость, при этом бизнес продолжает привлекать капитал для роста, масштабирования продаж, развития продукта и усиления команды. Важно, что такой формат не означает полного выхода фаундера из проекта. Напротив, покупатели и инвесторы, как правило, заинтересованы в сохранении ключевых основателей в капитале или управлении, поскольку именно команда часто является носителем продуктовой экспертизы и ключевым фактором успешной интеграции.

Более низкая распространенность инструментов заемного характера, включая акционерные и конвертируемые займы, также логична. В 2025 г. инвесторы были более сфокусированы на прямом участии в капитале, без увеличения долговой нагрузки и выплаты процентов. При этом pre-IPO структуры оставались релевантными, но скорее для ограниченного круга компаний с достаточным масштабом, прозрачной финансовой историей и понятной equity story для публичного рынка.

В целом результаты опроса подтверждают классический тренд — в сделках с технологическими активами всегда были распространены cash-in инвестиции, и 2025 г. не стал исключением. Для большинства бизнесов в сегменте tech, особенно тех, у которых отсутствует hardware-составляющая, equity-финансирование фактически является единственным источником фондирования по причине отсутствия залоговой массы.



Юлия Загорнова

партнер Группы компаний Б1

Б1 НОВЫЕ ВЫЗОВЫ НОВЫЕ РЕШЕНИЯ

Мы как консультант в своей практике видим, в основном, сделки, в которых входом в бизнес интересуется новый equity-инвестор, а продавцом выступает основатель бизнеса. При этом инвесторы в подавляющем большинстве случаев настаивают на cash-in, а продавцы хотят получить хотя бы какую-то часть суммы в виде cash-out. Договариваются стороны, как правило, в итоге о комбинации этих элементов в какой-то разумной пропорции. Это позволяет основателю и получить значимую сумму для реализации своих дальнейших жизненных планов, и не «перегрузить» бизнес деньгами, которые он не сможет сиюминутно эффективно освоить. По опыту сейчас сбалансированная комбинация выглядит как 70% cash-in и 30% cash-out. Раньше пропорция cash-out была выше, однако в нынешних экономических условиях инвестор видит необходимость понимать, куда идут его деньги.

43% участников опроса отметили, что часть сделок в сегменте tech наряду с привлечением equity-инвестиций и входом новых инвесторов была направлена на выход участников предыдущих раундов без cash-out'а основателя бизнеса. Это говорит о том, что в 2025 г. ряд финансовых инвесторов реализовали выход из ранее приобретенных активов. Некоторые из таких сделок совершались в том числе в формате tag-along, когда миноритарную долю текущего участника выкупал привлеченный им новый финансовый или стратегический инвестор. Одновременно он мог поучаствовать в сделке equity-финансирования компании путем внесения cash-in инвестиций. В ряде сделок доли инвесторов предыдущих раундов приобретались пулом текущих участников, без привлечения новых игроков в сделку выкупа.



Артем Тамаев

партнер корпоративной практики и M&A

BETTER CHANCE

Как показывает опрос, в 2025 г. при приобретении ИТ-компаний преобладали сделки с cash-in элементом. Эти результаты подтверждают наше видение рынка — любой инвестор желает разделить возможные бизнес- и юридические риски с новыми и историческими акционерами и направить новые средства на развитие бизнеса.

Опрос еще раз подтверждает тезис, что роль фаундера продолжает иметь краеугольное значение в построении ИТ-компании. Поэтому в случае, если сделка и предполагает какой-либо элемент cash-out фаундера, то в большинстве случаев фаундер не имеет возможности выйти полностью, чтобы обеспечить запрос нового инвестора на стабильность и дальнейшее развитие ИТ-компании.

Преобладание структур с cash-in элементом над другими формами финансирования свидетельствует о том, что любой инвестор желает получить определенные механизмы защиты своих инвестиций через участие в капитале (например, определенные права вето по существенным вопросам деятельности ИТ-компании), которые обычно достигаются через такие инструменты, как корпоративный договор и устав. Наличие таких средств также позволяет обеспечить более высокую ликвидность инвестиции инвестора, особенного в случае дальнейшего изменения состава участников ИТ-компании.



Анастасия Духина

старший юрист практики корпоративного права / M&A

sll

Наш опыт 2025 г. полностью подтверждает приведенные выше данные. В большинстве сопровождаемых нами сделок в качестве приобретателя выступали финансовые инвесторы (как правило, пул из 2–3 инвестиционных фондов или банков в любой комбинации), которые были заинтересованы в предоставлении денег самой компании на ее развитие и масштабирование, а также подготовке к IPO. Совсем небольшое число сделок (10%) совершалось приобретателями из технологического сектора (включая экосистемы), которые стремились закрыть потребность в определенном продукте / компетенциях или запустить новое направление с минимумом затрат и возможностью синергии с имеющимися продуктами и сервисами. При этом в последнем случае, если сделка предусматривала приобретение не сразу 100%, а постепенное увеличение доли приобретателя, достаточно остро вставал вопрос порядка и сроков интеграции приобретаемого бизнеса с имеющимся бизнесом покупателя. В таких случах в документах по сделке приходилось достаточно подробно прописывать вехи и контрольные точки интеграции в привязке к этапам увеличения доли приобретателя в таргете.



Кристина Мкртчян

советник практики интеллектуальной собственности

ЭБР Юридическая Компания

По оценке 81% респондентов, в 2025 г. cash-in был самой востребованной структурой при приобретении долей в российских ИТ-компаниях (синдикат новых инвесторов).

Почти сопоставимый результат получил смешанный формат cash-in и cash-out фаундеров (76% респондентов).

Это указывает на двойственную природу сделок Tech M&A на рынке: с одной стороны, компании продолжают нуждаться в капитале для роста, развития продукта и масштабирования, а с другой стороны, фаундеры и ранние участники чаще используют сделку не толь-

ко как инструмент привлечения финансирования, но и как механизм частичной фиксации уже созданной стоимости.

Мала популярность чистого конвертируемого займа (7% респондентов). Это может объясняться тем, что на более зрелых стадиях инвесторы предпочитают получать корпоративную позицию сейчас, а не откладывать вопрос оценки и контроля на будущее.

Интересно, что cash-out инвестора более раннего раунда отметили 43% респондентов. Это может говорить о постепенном усложнении cap-table российских технологических компаний: в сделках уже требуется учитывать интересы не только фаундеров и нового инвестора, но и прежних финансовых инвесторов, владельцев опционов, кредиторов и иных участников корпоративной структуры.

Видится, что Tech M&A все меньше похожи на простое приобретение доли и все больше требуют комплексной «пересборки» корпоративного и финансового контура таргета.



Владислав Лазуткин

старший юрист

ORION

Необходимо разграничивать венчурные / прямые инвестиции, которые предполагают cash-in, и собственно M&A сделки. Могу отметить, что модели M&A сделок, которые мне встречались, можно разделить на два типа в примерно равном соотношении (50 / 50): (i) cash-out либо (ii) комплексная модель, включающая (A) cash-in и выкуп долей ранних инвесторов и частичный выкуп долей фаундера (‘secondary investment’), (Б) опционы, позволяющие приобрести контроль над бизнесом, а также (В) инструменты корректировки размера доли стратегического инвестора (‘ratchet’).

Распространенные форматы сделок с технологическими активами в 2025 г.

В рамках одного из онлайн-опросов мы попросили участников отметить наиболее популярные, по их мнению, форматы приобретения участия в активах при реализации проектов Tech M&A в 2025 г. Результаты опроса приведены ниже.

#РЕЗУЛЬТАТЫ_ОПРОСОВ

Какие форматы приобретения ИТ-активов вы чаще использовали в 2025 г.?



6%

Создание стратегического альянса с российскими или зарубежными ИТ-партнерами на основе договорной обвязки (без формирования юридического лица)

4%

Asset-deal — приобретение крупного пула ИТ-активов российской компании без покупки долей компании

По данным Опроса по структурированию сделок Tech M&A в 2025 г. (125 респондентов).

Как показали результаты опроса, в 2025 г. преобладающим форматом участия в IT-компаниях стало **приобретение пакета в диапазоне 35–49%**, то есть т. н. «пакета существенного влияния» (**78% респондентов**). Также в 2025 г. часто совершались сделки приобретения контролирующих долей (включая сделки по реализации ранее заключенных опционов) (**66% респондентов**)и сделки приобретения пакетов «негативного контроля» (**62% респондентов**).

Многие эксперты, опрошенные нами в ходе проведения исследования, отметили, что, по их оценкам, средний размер долей, приобретенных стратегическими инвесторами в 2025 г., находился в диапазоне 35–49%. Такой пакет участия позволял инвесторам оценить потенциал синергий и комплементарность активов, ограничивая при этом уровень риска. Подобные сделки часто сопровождались опционами-колл, позволяющими увеличить размер участия в будущем. В условиях повышенной неопределенности формат «существенного влияния» стал для стратегов оптимальным решением, сочетающим инвестиционные возможности, балансировку ценовых ожиданий и гибкость в управлении рисками.



Вячеслав Поджаров

старший менеджер проектов

ADVANCE CAPITAL

Рынок Tech M&A в 2025 г. не был сосредоточен вокруг одного доминирующего формата контроля. Инвесторы таргетировали долю в зависимости от их целей и типа инвестора. Финансовые инвесторы — миноритарные пакеты, стратегические инвесторы — от блокирующих долей до контроля. Такая в целом картина отражает специфику технологических активов: стратегическому покупателю зачастую важно не просто получить формальный контроль над юридическим лицом, а выстроить рабочую модель партнерства с фаундерами и ключевой командой.

Высокая доля сделок с существенными миноритарными пакетами объясняется тем, что многие инвесторы стремились получить долю в капитале с потенциалом роста капитализации, в т. ч. в рамках Pre-IPO формата сделок. Для технологического бизнеса такой формат часто оказывается сбалансированным: основатели сохраняют контроль и мотивацию развивать бизнес, инвестор получает влияние на ключевые решения.

Значительная доля сделок с контролем со стороны стратегических инвесторов показывает, что покупателям было важно обеспечить полную управляемость актива. Это особенно важно в контексте интеграции в существующую технологическую платформу, инфраструктуру или клиентский контур покупателя. Низкая доля asset-deal структур также показательна для этого сектора. В ИТ стоимость редко сосредоточена только в отдельных активах / IP. Как правило, это комплекс условий, связанных с командой, кодом, клиентскими отношениями, данными, продуктовой экспертизой, которые сложнее отделить от юридического лица без потери части ценности.



Юлия Загорнова

партнер Группы компаний Б1

Б1 НОВЫЕ ВЫЗОВЫ НОВЫЕ РЕШЕНИЯ

В прошлом году мы видели в основном две категории сделок, зависящие от структуры покупателя. Если в ИТ-компанию инвестировал независимый инвестиционный фонд, то чаще всего речь в сделке шла о приобретении миноритарной доли до 25% с целью дальнейшей совместной продажи бизнеса крупному стратегическому игроку или выхода на IPO в среднесрочной перспективе.

Альтернативно мы видим сделки, где инвесторам важна консолидация бизнеса в своей отчетности. При этом инвестор понимает риски, связанные с возможной переплатой за бизнес в случае невыполнения заявленных планов, и хочет их минимизировать. В этом случае речь в ходе сделки идет о приобретении 51% долей на первом этапе с последующим выкупом долей до 80–100% в зависимости от структуры собственности приобретаемой компании, а также участия в ней текущего менеджмента, что для инвесторов все чаще становится особенно важно для достижения заявленных результатов. В некоторых ситуациях новый инвестор сам предлагает включить текущий менеджмент в состав миноритарных акционеров, если до сих пор этого не было сделано, с целью формирования правильной мотивации для дальнейшего развития бизнеса.

В то же время мы стали чаще встречаться с ситуациями, в которых стратегический инвестор, приобретая контроль, не стремится выкупить 100% долей, а готов видеть основателя компании миноритарным акционером на 20–25% на постоянной основе.

Многоэтапные сделки

В 2025 г. продолжил развитие тренд на **поэтапный вход стратегических инвесторов** в технологические активы. Однако, в отличие от предыдущих лет, в 2025 г. на первой стадии входа в актив большинство инвесторов приобретали не контролирующую долю, а пакеты меньшего размера участия. Это обусловлено рядом причин.

Во-первых

Как уже отмечалось ранее, стратегические инвесторы в 2025 г. **более осторожно принимали новые инвестиционные решения** и сфокусировались на поддержании текущих проектов. Вход в новые активы стал более фокусным и адресным, проверка гипотез и тестирование синергий — более тщательными. Решения о консолидации активов с перераспределением контроля принимались преимущественно в отношении инвестиций, совершенных до 2025 г., если в отношении них подтверждались заявленные результаты, возможность реализации синергий и прикладные эффекты.

Для оценки эффективности новых активов в 2025 г. приобретателям **не требовался пакет участия, включающий полный набор инструментов стратегического контроля**. Многим игрокам было достаточно полномочий, позволяющих влиять на принятие ряда значимых решений, в том числе на операционном уровне.

Такая позиция требовала тонкой настройки и гибкого баланса интересов в вопросах корпоративного управления и операционного развития актива. При этом формальный контроль сохранялся за владельцем бизнеса, что способствовало более быстрому достижению компромисса между сторонами.

Во-вторых

Владельцы зрелых и финансово устойчивых активов, обладающие более сильной переговорной позицией, не всегда были готовы уступить стратегическому покупателю контрольные полномочия на первом этапе сделки. Особенно если в отношении них устанавливались строгие КПЭ, влияющие на итоговый размер цены, а покупатель при этом настаивал на существенной рассрочке оплаты.

В-третьих

Большинство покупателей, вне зависимости от размера приобретаемого пакета и силы переговорной позиции, стремились к тому, чтобы обеспечить больший объем полномочий на уровне договорных инструментов и договориться о поэтапной оплате. Поэтому нередко на первом этапе сделки, особенно при покупке качественных активов, им приходилось выбирать между ценой и размером пакета / объемом полномочий. Во многих случаях покупатели уступали позиции продавца и ограничивали долю участия, приобретаемую при входе в актив, размером пакета ниже контрольного.



Мария Ларионова

юрист корпоративной практики и M&A

BETTER CHANCE

Результаты опроса подтверждают наше наблюдение, что за предыдущий год значительную долю Tech M&A-сделок составило приобретение инвесторами существенных миноритарных долей.

Приобретение такого пакета в совокупности с использованием договорных механизмов позволяет инвесторам «кастомизировать» характер и степень своего участия в управлении активом и контроле за наиболее существенными решениями. Эта тенденция связана как с тем, что в условиях волатильного рынка инвесторы стали менее открыты к риску, так и с их желанием выстраивать полноценное долгосрочное партнерство с возможным расширением своего участия в зависимости от финансовых показателей приобретаемого бизнеса.

Распространен сценарий многоэтапной сделки, где приобретение существенного миноритарного или блокирующего пакета — это первый шаг, после которого инвестор получит возможность изнутри оценить маржинальность и перспективы актива, чтобы впоследствии продать или увеличить свою долю. Это преимущественно реализуется с использованием сложноструктурированных корпоративных договоров, а также опционных конструкций.

В подобных сделках требуются нестандартные решения для отражения коммерческих договоренностей сторон в силу многих особенностей ИТ-бизнеса: сложности при проверке и оценке ключевых активов, существенной роли персонала, риска снижения стоимости актива на фоне стремительного развития ИТ-рынка и продуктов конкурентов и др.

Приобретение контроля и тренд на создание СП

Как показали итоги опроса, доля сделок, опосредующих приобретение **контрольных пакетов** в технологических компаниях, в 2025 г. также была существенной. В 2025 г. такие сделки происходили как в результате реализации опционов-колл, то есть в рамках имплементации последующего этапа сделки, заключенной до 2025 г., так и при первичном входе в бизнес.

В прошлом году большинство инвестиционных решений о покупке контроля в новом активе принималось не по итогам первичной оценки и due diligence, а по результатам тщательной проверки качества и устойчивости бизнеса в рамках первого, более раннего этапа приобретения. Однако, как отмечают эксперты рынка, сделки по консолидации активов (в том числе до размера квалифицированного контрольного пакета) в рамках последующих этапов, которые пришлись на 2025 г., как путем реализации опциона, так и новой договоренности, в прошлом году не сформировали значимого тренда.

Большая доля сделок по покупке контроля (как квалифицированного, так и простого) в 2025 г. была сконцентрирована на первых этапах реализации проектов по приобретению новых активов. Во многих из таких случаев инвесторы были хорошо знакомы с активом, например, в результате участия в партнерских альянсах или долгосрочной контрактации с таргетом-вендором на операционном уровне без участия в структуре его капитала. При этом, как было отмечено ранее, среди общего числа проектов Tech M&A 2025 г. доля сделок по покупке контроля (как в рамках первичной, так и вторичной сделок) не являлась преобладающей, уступая место приобретению крупных миноритарных пакетов.

В результате такого перераспределения частного капитала на рынке Tech M&A в 2025 г. закрепился **тренд на формирование т. н. «неклассических» СП**, в которых доля lead-участника могла существенно превышать 50%, а оставшаяся часть капитала — быть распределенной между пулом миноритарных инвесторов. Во многих случаях партнером с преобладающим участием в рамках СП становился стратегический инвестор, являющийся основным «кандидатом» на консолидацию всего актива в будущем.

Динамика в сторону роста доли СП в структуре рынка Tech M&A начала развиваться еще до начала 2025 г., в прошлом году этот тренд укрепился. Это обусловлено в том числе стремлением стратегических инвесторов и крупных технологических партнеров распределить риски в условиях повышенной неопределенности, даже если актив потенциально интересен для полной интеграции, что соответствует ранее отмеченным тенденциям.

Сделки с классическими СП, предполагающими паритетное или около-паритетное участие партнеров, в 2025 г. также составляли значительную долю среди проектов, особенно капиталоемких, в сегменте tech (чуть более четверти всех сделок по результатам опроса).



Софья Смирнова

советник M&A
и корпоративной практики

O_2 консалтинг

Примечательное в этих цифрах, как представляется, не перевес сделок с миноритарной долей (в разной конфигурации) сам по себе, а предпочтение неконтрольной доли доле, дающей формальное простое большинство голосов. Переход за 50% долю включает презумпцию контроля и консолидацию в отчетности, тогда как сам бизнес часто продолжают вести основатели. Традиционно сделки структурируются через «негативный контроль» за конкретными операциями бизнеса в корпоративном договоре, часто преобладают структуры поэтапного входа в капитал.

Та же логика объясняет и второе следствие распределения голосов: контроль, если все-таки его получать, покупатели предпочитают квалифицированный. 78% и 66% в сумме дают заметно больше ста — значительная часть респондентов делала и покупку существенной миноритарной доли, и покупку квалифицированного контроля. Это совпадает с тем, что мы видим в практике: миноритарный вход и квалифицированный выкуп — скорее не конкурирующие стратегии, а стадии одной. Типовая конструкция — существенная миноритарная доля с колл-опционом, привязанным к финансовым или продуктовым метрикам таргета. Для ИТ-сектора это выглядит органично: стоимость актива создают основатели и команда, и немедленный выкуп 100% может разрушить мотивацию тех, кто эту стоимость генерирует.

Сама по себе доля в капитале еще не означает комплексной защиты прав — лучшие практики защиты в большинстве случаев находят отражение в корпоративном договоре. Как правило, это вето по ключевым вопросам, система «сдержек и противовесов» в виде опционных конструкций и прав tag / drag. Но у договорной обвязки есть предел: по общему правилу нарушение корпоративного договора дает убытки и неустойку, оспорить решение органа общества можно, лишь если сторонами договора были все участники общества, а сделку — если контрагент знал или должен был знать об ограничениях (п. 6 ст. 67.2 ГК); третьих лиц SHA не обязывает. Поэтому юридически устойчи-

вая защита достигается переносом ключевых договоренностей из SHA в устав: фиксирование квалифицированного большинства или единогласия по ключевым вопросам дает миноритарию блокирующую силу против всех, а не только против сторон договора, — нарушение уставных порогов влечет недействительность решения. В ООО к этому добавляются дополнительные права участника (ст. 8 ФЗ об ООО). Зеркально и покупатель контроля решает ту же задачу размером пакета: квалифицированная доля снимает риск блокировки по квалифицированным вопросам из закона.

Низкие доли альянсов (6%) и asset-deals (4%) — две стороны одной особенности ИТ-актива: он не отделяется от юридического лица без потерь. Договорная обвязка без капитала не дает консолидации. Карваут требует переоформления прав на РИД, согласий лицензиаров, расходов на перевод команды и, в отличие от продажи долей, облагается НДС. Юрлицо покупают потому, что оно эффективно опосредует отчуждение ИТ-актива.



Артем Асоян

юрист

ORION

> В 2025 г. мы встречали сделки, в которых стратегический инвестор приобретал мажоритарный пакет без опционов на последующий выкуп оставшихся акций / долей или обратную продажу своего пакета с целью совместного развития бизнеса (без какой-либо интеграции таргета в периметр инвестора) и исключительно для выхода на стратегическую продажу обоих акционеров / участников в обозримом будущем.

Реструктуризация периметра владения

Под влиянием усиливающегося санкционного давления в 2025 г. продолжили совершаться сделки по реструктуризации международных IT-компаний, имеющих присутствие в России, с целью разделения глобального бизнеса на локальный и зарубежный контуры. Их доля среди общего числа сделок Tech M&A была невелика, так как большая часть глобальных игроков к 2025 г. уже ушла с российского рынка. Такие проекты крайне сложны с точки зрения юридического структурирования, требуют согласования с регуляторами, а также координации работы и взаимодействия с командами зарубежных консультантов и специалистов из смежных областей. Проведение подобной реструктуризации является предварительным этапом реализации сделок по выходу международного игрока с российского рынка с закрытием локального сегмента или его продажей другому игроку.



Сергей Еремин

партнер

NIKOLSKAYA consulting



Анна Ивонина

юрист

NIKOLSKAYA consulting

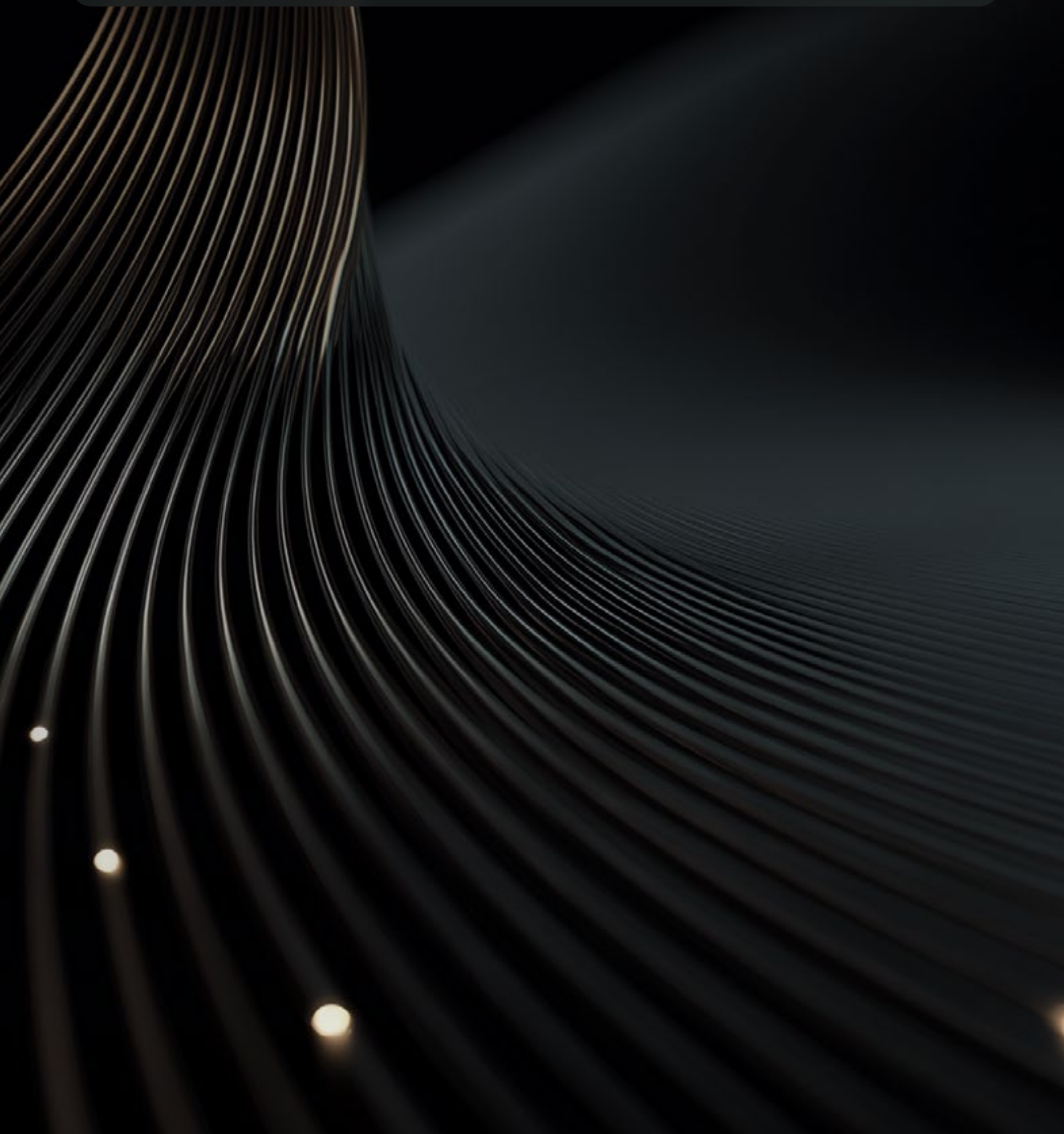
Санкционные аспекты становятся ключевым фактором реструктуризации международного IT-бизнеса. На практике мы выделяем несколько критически важных элементов, которые учитываются при структурировании и реализации подобных сделок.

Во-первых, поставки иностранного ПО и экспортный контроль. В условиях масштабного санкционного давления компании часто вынуждены использовать сложные цепочки поставок и разделять IT-бизнес на российскую (санкционно «токсичную») и зарубежную части. Сделки с иностранными поставщиками обычно проводятся через «нетоксичную» зарубежную компанию. Однако этого недостаточно: для минимизации рисков необходимо публично и операционно дистанцировать зарубежный бизнес от российского, чтобы у контрагентов не возникало сомнений относительно соблюдения санкционных режимов. Важную роль здесь играет PR-стратегия, направленная на демонстрацию рынку, партнерам и регуляторам того, что зарубежная часть очищена от санкционного следа и не создает правовых рисков для контрагентов.

Во-вторых, персональные риски бенефициаров и топ-менеджеров. Регуляторы США и ЕС внимательно отслеживают российский IT-сектор, рассматривая даже гражданские технологии как потенциально имеющие двойное назначение, а также учитывая взаимодействие компаний с государственными структурами. Наличие санкционных рисков не означает автоматический запрет сделки, однако при участии иностранного подписанта рекомендуется его дистанцирование от согласования сделки и подписания документов. В противном случае возрастает риск нарушения санкций и привлечения к уголовной ответственности.

В-третьих, взаимодействие с силовыми структурами в рамках обязательных требований законодательства или публичных мероприятий создает риск вторичных санкций. Юридическая стратегия строится на жестком операционном разделении функций: российская часть выполняет локальные требования, тогда как международная изолируется от доступа к чувствительным данным.

Наконец, экосистемные риски. Современные IT-платформы глубоко интегрированы с внешними сервисами, включая API, облачные решения и платежную инфраструктуру. В рамках due diligence анализируется вся цепочка вендоров и интеграций клиента.



Раздел 3

Структурирование и управление рисками в сделках с технологическими активами

Практика 2025 г.

АВТОРЫ



Анастасия Нерчинская



Александр Панов
VERBA LEGAL



Роман Головацкий
DENUO

Краткие выводы

- В 2025 г. переговорный баланс и расстановка приоритетов в сделках с технологическими активами отражали общую динамику «рынка покупателя». Это предопределило изменение стратегии Tech M&A-процесса — в структурировании сделок акцент существенно сместился в сторону использования подходов, защищающих интересы инвесторов.

- В условиях высокой стоимости финансирования, сложной макроэкономической ситуации и неопределенности прогнозов покупатели стали тщательнее анализировать качество активов и чаще использовать инструменты, обеспечивающие защиту инвестиций, возврат доходности, реальную возможность привлечения продавца к ответственности за дефекты актива и беспрепятственный выход из сделки в случае реализации неблагоприятного сценария.

- Большинство экспертов отметили, что в 2025 г. процессы переговоров и структурирования сделок Tech M&A стали более длительными и сложными. Необходимость сближения разнополярных интересов сторон и, в первую очередь, разногласий по вопросам оценки потребовала более тщательного выбора юридических инструментов, обеспечивающих принципиальную возможность достижения компромисса по условиям сделок. Ряд экспертов отметили тренд использования в рамках одной сделки отдельных инструментов, характерных для разных типов инвестиций, — VC или PE, классического СП, стратегического M&A.

- В Tech M&A проектах с участием стратегических покупателей стандартной практикой стали поэтапные входы в актив с использованием сложных механизмов перераспределения контроля «внутри» сделки, включая механики earn-out и «рэтчеты». Переговоры часто сфокусировались на согласовании размера пакета первичного входа инвестора и его балансировке набором корпоративных прав, а также величиной первого платежа. Продавцы качественных активов реже уступали операционный контроль на первом этапе сделки, особенно, если первый транш составлял менее 60–70% ожидаемой цены. При этом покупатели по-прежнему стремились получить максимум контрольных полномочий при входе в актив, встроить в сделку механизмы отложенного платежа и согласовать стоимость первого транша без учета премии за контроль.

- Две наиболее распространенные механики структурирования сделок Tech M&A — earn-out (отложенный платеж, обусловленный достижением согласованных КПЭ) и holdback (удержание части цены, обеспечивающей защиту на случай материализации исторических рисков), — в 2025 г. не просто сохранили актуальность, но и нередко использовались одновременно, обеспечивая мотивацию роста бизнеса и «страховку» от текущих рисков.

- В сделках Tech M&A 2025 г. большое внимание традиционно уделялось вопросам, связанным с удержанием и мотивацией менеджмента и технической команды, предотвращением переманивания ключевых работников и создания конкурирующих бизнесов. Инвесторы фокусировались на поиске эффективных механизмов, позволяющих обеспечить удержание команды после закрытия сделки в отсутствие у них прямых инструментов влияния на эти процессы.

- В 2025 г. в сделках Tech M&A чаще использовались штрафные опционы в качестве инструмента балансировки поведения миноритарных участников, включая основателей, сохранивших долю в капитале, и их мотивации на обеспечение финансовой и операционной дисциплины в активе.

- Компенсационные механики также стали более сложными — все чаще в сделках использовалась концепция заранее оцененных убытков, позволяющая перенести бремя доказывания размера убытков на продавца.

- Многие эксперты отметили, что в 2025 г. усложнились процессы предпродажной реструктуризации технологических активов. Прединвестиционная реструктуризация бизнеса чаще становилась отлагательным условием закрытия сделок. Большего вни-

мания требовали не только традиционные вопросы «пересборки» контура активов, но и необходимость более тщательной проработки отношений с инвесторами предыдущих раундов, «расшивки» долгов, прекращения ранее выданных опционов, «выравнивания» таблицы капитализации и прочих договоренностей предыдущих стадий, их синхронизации с условиями новой сделки и разными стратегическими целями инвесторов.

- В сделках Tech M&A, как и прежде, инвесторы стремились предотвратить размытие стоимости бизнеса до закрытия сделки, в том числе путем оптимизации механик закрытия расчетов (locked box, completion accounts, гибриды), использования инструментария «обязательств до закрытия сделки» (pre-closing conduct) и других инструментов. В сделках сегмента high-market в 2025 г. нередко использовались механики completion accounts, а в проектах mid-market более распространенным являлся механизм locked box.

Следуя общим трендам на рынке M&A, сегмент сделок с технологическими активами в 2025 г. продемонстрировал смещение переговорного и стратегического баланса в сторону покупателей. Подходы к юридическому структурированию проектов Tech M&A в 2025 г. отразили эту тенденцию. В сделках с технологическими компаниями преобладали «пропокупательские» стратегии, направленные на минимизацию исторических рисков и, в то же время, — мотивирующие команду на обеспечение роста стоимости бизнеса.

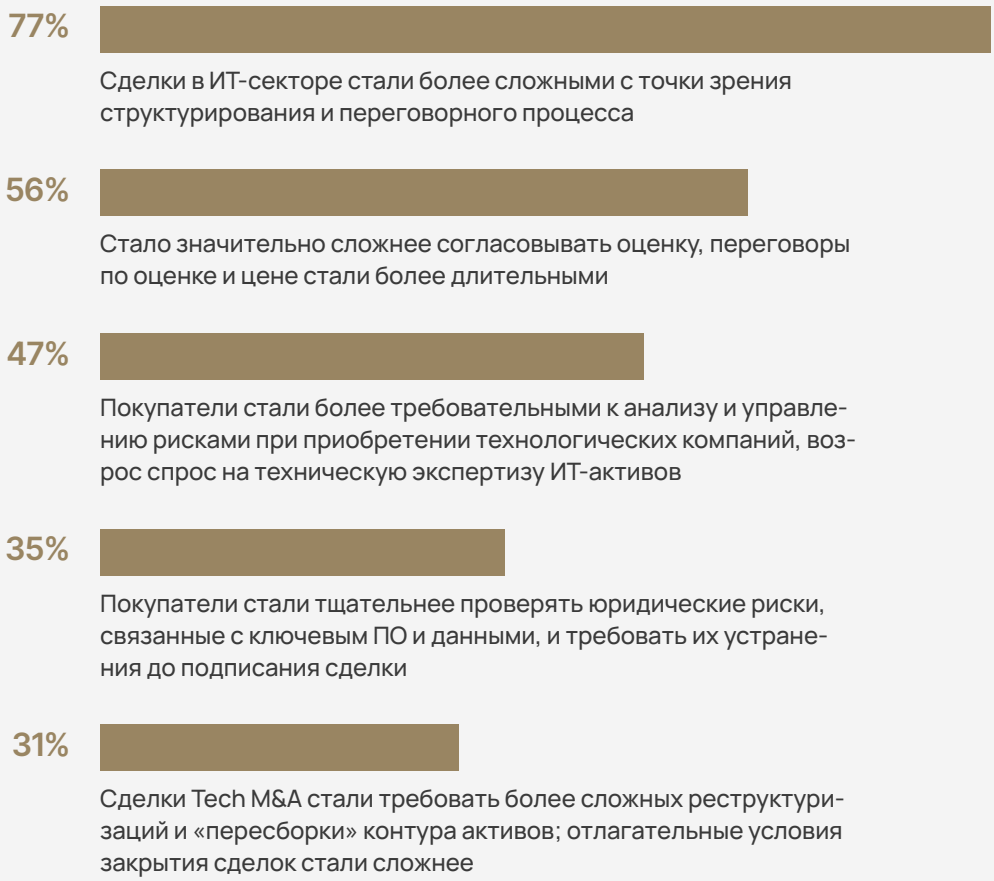
Большинство Tech M&A экспертов, опрошенных нами в ходе проведения исследования, отметили, что в 2025 г. процесс сопровождения сделок в сегменте tech стал существенно сложнее на всех его этапах — от согласования оценки до выбора инструментов распределения рисков. Наиболее ярко это проявилось в сделках с качественными активами, имеющими подтвержденные финансовые результаты и минимальный уровень долговой нагрузки, где логика «рынка покупателей» не была линейна и требовала от сторон гораздо больше гибкости.

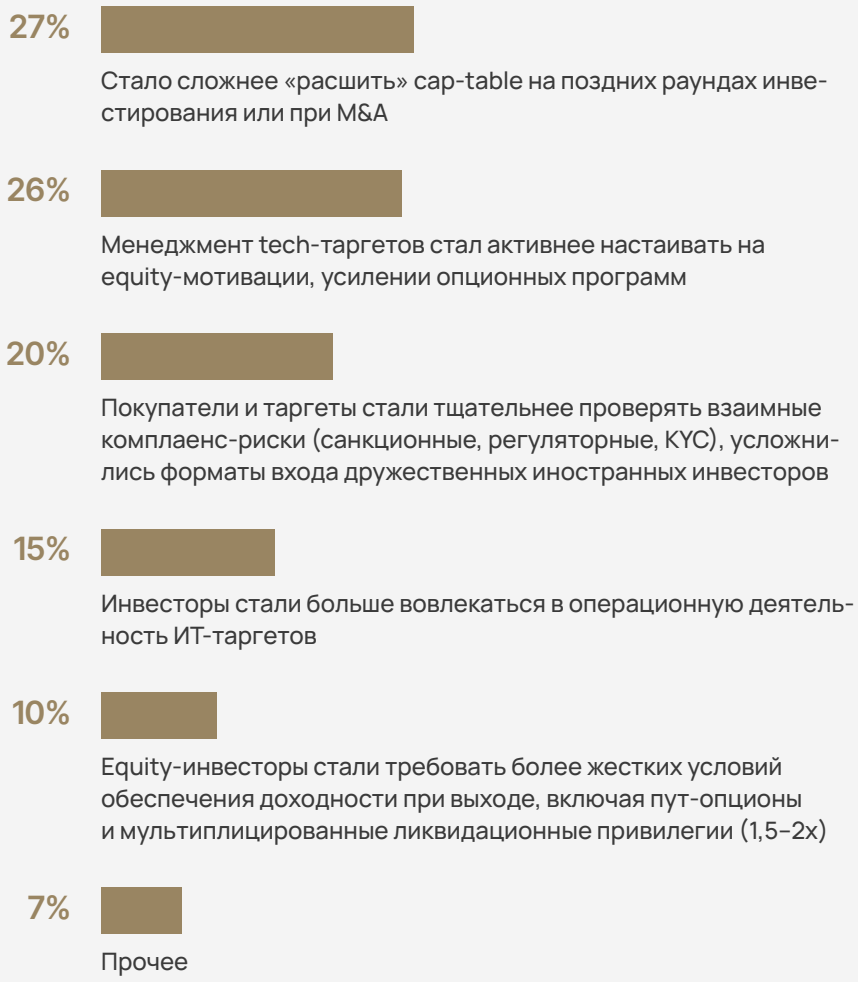
3.1 Наиболее сложные вопросы переговоров по сделкам Tech M&A 2025

В ходе онлайн-опроса мы попросили экспертов отметить особенности и сложности, с которыми они столкнулись в рамках переговорного процесса и структурирования сделок Tech M&A в 2025 г.

#РЕЗУЛЬТАТЫ_ОПРОСОВ

Особенности и сложности ведения переговоров и структурирования сделок в 2025 г.





По данным Опроса по структурированию сделок Tech M&A в 2025 г. (125 респондентов).

Результаты опроса подтверждают развитие **в 2025 г. тренда на усложнение переговорного процесса и структурирования сделок Tech M&A** и переход инвесторов к стратегиям минимизации риска, включая их максимальное перераспределение на продавца уже «внутри» сделки. В 2025 г. центральной проблемой транзакционного процесса в сегменте tech стал поиск баланса между различными взглядами сторон на текущую оценку бизнеса, потенциал ее роста, «понятность» синергий и уровень исторических рисков.

Форматы и решения в логике «простой и быстрой» сделки в 2025 г. все чаще отклонялись покупателями по итогам оценки и due diligence как неэффективные и не способные привести стороны к компромиссу. **Поэтапная передача покупателю контроля** над активом стала базовым сценарием структурирования, позволяющим, в том числе, сгладить проблему конфликта мотиваций в модели earn-out. В 2025 г. эта механика, ставшая транзакционным стандартом, **потребовала более тонкой настройки**. «Ступенчатую» передачу участия в капитале актива часто необходимо было синхронизировать с рассрочкой платежей, при которой размер первого транша мог не соответствовать стоимости объема реально передаваемых контрольных полномочий.



Вячеслав Поджаров

старший менеджер проектов

ADVANCE CAPITAL

Все стороны отметили, что сделки в Tech M&A стали заметно более сложными как с точки зрения переговорного процесса, так и с точки зрения структурирования. На фоне высокой стоимости капитала, более осторожного отношения к рискам и разрыва ожиданий по оценке стороны стали дольше обсуждать не только цену, но и то, за счет чего эта цена должна быть подтверждена. В центре переговоров все чаще оказывались качество выручки, устойчивость клиентской базы, технологическая состоятельность продукта, зависимость от ключевой команды и возможность интеграции актива в бизнес покупателя.

Отдельно стоит отметить рост роли технической экспертизы. Для покупателей стало недостаточно получить финансовую модель, презентацию и стандартный набор юридических документов. В технологических сделках важно понять, насколько заявленные характеристики продукта соответствуют реальному состоянию кодовой базы, архитектуры, инфраструктуры и процессов разработки. Поэтому technical due diligence постепенно становится не дополнительной проверкой, а одним из ключевых элементов инвестиционного решения.

Усложнение переговоров также связано с тем, что в ряде сделок требовалась предварительная «пересборка» периметра: перенос прав на ПО, урегулирование отношений с разработчиками, структурирование опционных программ, очистка cap table, фиксация прав на данные и корректное оформление отношений с ключевыми клиентами. Чем более зрелым становится рынок, тем выше требования покупателей к качеству подготовки актива. Для продавцов это означает, что успешная сделка все чаще начинается заранее — с подготовки и закрытия потенциальных рисков.



Юлия Загорнова

партнер Группы компаний Б1

Б1 НОВЫЕ ВЫЗОВЫ НОВЫЕ РЕШЕНИЯ

В 2025 г. вопросы оценки все чаще становились камнем преткновения в силу меньшей, чем ранее, готовности инвесторов идти на риск возможной переплаты за актив, что объяснялось высокой ключевой ставкой и наличием менее рисковых, но зачастую ненамного менее доходных инструментов для инвестирования. «Сшивать» позиции сторон приходилось за счет формирования более сложных и многоступенчатых конструкций в структуре сделки — earn-out и рэтчет уже никого не удивляют и давно стали нормой структурирования сделок в ИТ-сегменте.

Жаркие дискуссии при этом разгораются и при обсуждении корпоративных прав сторон. Особенно когда приобретается контрольная доля, но при этом есть «хвост» в виде earn-out, и продавец, естественно, хочет контролировать исполнимость согласованных КПЭ, к которым привязаны финальные расчеты по сделке.



Алексей Мустяца

директор, управление слияний и поглощений

СОВКОМБАНК

Итоги опроса о росте сложности структурирования сделок Tech M&A в 2025 г. полностью соответствуют нашей практике. Сделки действительно стали более сложными как на этапе переговоров, так и с точки зрения юридической конструкции, прежде всего из-за роста требований к управлению рисками и необходимости учитывать регуляторные, санкционные и технологические факторы.

В 2025 г. в ряде сделок требовалась предпродажная реструктуризация и консолидация контура ключевых активов, в том числе прав на ПО и данные. Наиболее сложными аспектами такого процесса являлись «очистка» IP-периметра, выведение ИТ-разработки в единый юридический контур и устранение исторических дефектов IP-assignment. В сделках с иностранным элементом дополнительную сложность создавали ограничения трансграничного характера и санкционный контур.

Механика earn-out в 2025 г. применялась существенно чаще и использовалась не только как инструмент ценообразования, но и как способ митигации рисков. Earn-out в нашей практике привязывался к финансовым и операционным KPI (выручка, EBITDA, удержание ключевых клиентов или команды), устанавливался на ограниченный период и сопровождался детальной регламентацией порядка расчета показателей. Наиболее сложными являлись вопросы контроля над бизнесом в период earn-out, доступа покупателя к информации и предотвращения конфликтов интересов. В отдельных случаях earn-out комбинировался с опционами или отложенными правами на доли.

Также в 2025 г. чаще использовались формульные механизмы корректировки цены, в том числе связанные с финансовыми показателями, долговой нагрузкой или выявленными рисками по результатам due diligence. Такие механизмы сочетались с заверениями и гарантиями, indemnity и иными инструментами защиты покупателя.

В целом исходя из нашей практики можно отметить, что в 2025 г. покупатели стали существенно более требовательными к митигации рисков, особенно в части privacy, прав на ПО и данных. Это напрямую влияло на структуру сделок, набор отлагательных условий закрытия и объем обязательств сторон, а юридическое структурирование все чаще становилось ключевым элементом успешного закрытия сделки.



Кристина Мкртчян

советник практики интеллектуальной собственности

ЭБР
Юридическая Компания

Результаты опроса подтверждают общий тренд на усложнение сделок в ИТ-секторе: 77% респондентов указали, что сделки стали сложнее и с позиции структурирования, и с позиции переговорного процесса.

Выделяется проблема оценки: 56% респондентов отметили, что стало сложнее согласовать оценку, начиная с раунда A и выше, а расчеты все чаще структурируются через earn-out.

Это и логично, потому что стоимость технологического бизнеса часто зависит не только от текущей выручки, но и от будущей масштабируемости продукта, качества команды, защищенности IP, устойчивости клиентской базы и регуляторной применимости технологии.

Поэтому earn-out выглядит как своего рода компромисс: продавец сохраняет возможность получить цену, соответствующую ожиданиям роста, а покупатель снижает риск переплаты за прогнозы, которые могут не реализоваться.

Логика «рынка покупателя» изменила переговорный баланс при согласовании ценовых условий и подходов к распределению рисков в пользу позиции инвесторов.

«Точки разногласий» и поиск компромисса

Механика **earn-out в 2025 г. закрепила свою роль в качестве базового стандарта сделок Tech M&A вне зависимости от ценового диапазона**. Согласовать «на берегу» итоговую стоимость бизнеса (EV) часто не удавалось из-за кратного расхождения кейсов продавца и покупателя и их позиций в отношении потенциала роста и динамики ключевых операционных метрик.

Однако в 2025 г. **существенно усложнилась реализация такого механизма**. Покупатели все реже были готовы приобрести корпоративный контроль на первом этапе сделки и ожидаемо настаивали на максимальной рассрочке платежа. При этом для целей проверки гипотез и реализации оставшейся части сделки — уже при входе в бизнес они требовали предоставления **существенного объема корпоративных прав**, включая возможность активно влиять на операционные процессы. Продавцы же, наоборот, при использовании модели earn-out не были мотивированы передать покупателю контрольные полномочия на первом этапе сделки, особенно если размер первого платежа был существенно ниже ожидаемого. «Блокирующий» пакет корпоративных прав продавцов в такой ситуации обычно не устраивал. Наиболее остро эта проблема касалась объема прав в части **операционного управления активом, от наличия которых напрямую зависели решения по КПЭ**, определяющие последующие выплаты.

При наличии в сделке других участников, включая инвесторов предыдущих раундов, или при входе в сделку нескольких инвесторов, например, финансового и стратегического, критично осложнялась синхронизация общего объема договоренностей. Поиск эффективного решения лежал в области юридического структурирования и требовал от команд особой гибкости и выработки нетривиальных подходов к использованию различных транзакционных инструментов, что занимало длительное время.

> **Поэтапная передача покупателю контроля над активом стала базовым сценарием структурирования сделок Tech M&A. Такой подход позволял сгладить проблему конфликта мотиваций в модели earn-out, давно ставшей транзакционным стандартом в сегменте tech, но потребовавшей в 2025 г. более тонкой настройки.**

Исторические риски в 2025 г. все чаще «закрывались» с помощью механики **holdback** — отсрочки платежа части цены, в отношении размера которой у сторон отсутствовали разногласия. Она все чаще **сочетала элементы отложенного платежа** (заранее известной его части, например, доли первого транша) на случай материализации рисков и классических **компенсационных механизмов**, таких, как заверения и имущественные потери.

В ряде случаев продавцы, остро нуждающиеся в инвестициях, соглашались на предоставление покупателю дискреции одностороннего (не требующего просуживания) уменьшения цены в пределах удерживаемой суммы на основании согласованной сторонами методики расчета параметров формулы. Однако чаще возможность уменьшения цены в модели holdback была «увязана» с обязанностью продавца **компенсировать подтвержденные судом убытки (особенно возникшие в связи с претензиями третьих лиц)** или имущественные потери покупателя и структурировалась через механизм зачета встречных требований. Особая сложность заключалась в необходимости **синхронизации механики earn-out**, при которой итоговый размер цены на момент закрытия сделки не известен, **и модели отложенного платежа**, «страхующего» от исторических рисков, применимой к уже определенной части цены.

Еще одной сложной задачей переговорного процесса являлся поиск оптимального решения в отношении **контроля команды и ее удержания** в бизнесе после закрытия сделки. В отсутствие у инвестора каких-либо эффективных инструментов влияния на HR-вопросы, а также в силу известных ограничений регуляторного характера эта проблема разрешалась преимущественно через **инструменты косвенной мотивации** на уровне продавца, сохраняющего долю в капитале.

Требование по удержанию ключевых кадровых позиций в течение согласованного срока после закрытия сделки **все чаще становилось самостоятельным** (а в некоторых случаях и единственным, что является небесспорной пратикой, так как сохранение персонала не позволяет определить размер прироста стоимости бизнеса и само по себе не обеспечивает его) **КПЭ в рамках механики earn-out**. В 2025 г. для этих целей стали чаще использовать дефолтные опционы-пут «на продавца», позволяющие инвестору скорректировать стоимость актива в случае увольнения команды.

Также в 2025 г. в сделках Tech M&A более «остро» обсуждались **вопросы объема ответственности продавца**. Распространение практики сочетания в рамках единой сделки элементов cash-in и cash-out потребовало особой точности юридических формулировок при согласовании **общего предела ответственности** и структурирования различных средств правовой защиты, особенно **механики уменьшения покупной цены в связи с дефектами актива**. Еще одной «болевой точкой» переговоров стали вопросы, связанные с режимами **наследования и общей собственности** в отношении долей физических лиц, возможность распоряжения которыми была структурирована в рамках сделки на будущее время. В первую очередь, эта проблема затрагивает опционные конструкции. Это особенно актуально в связи с развитием в 2025 г. тренда на создание СП в сегменте tech, сторонами которых часто являются физические лица — основатели IT-бизнесов.

В ходе исследования мы попросили ведущих M&A-консультантов рассказать о том, согласование каких вопросов, обсуждаемых на переговорах по сделкам Tech M&A в 2025 г., вызывало наибольшие сложности и требовало значительных усилий для достижения компромисса.



Арташес Оганов

партнер, глава практики корпоративного права / M&A



Анастасия Духина

старший юрист практики корпоративного права / M&A

Наиболее сложным при сопровождении технологических сделок в 2025 г. было достижение компромисса между продавцом и покупателем по нескольким ключевым аспектам сделки:

1. **Момент оплаты покупной цены и ее размер**. Если продавцы в сопровождаемых нами сделках ожидали получить не менее 75% покупной цены до перехода долей или на закрытии, то покупатели, наоборот, были не готовы к таким суммам и стремились отстоять возможность оплаты либо всей суммы после перехода долей либо в несколько этапов со значительной частью по earn-out (как правило, 50/50% или 60/40%);
2. **Сохранение контроля продавца над бизнесом**. Этот «камень преткновения» характерен для сделок, где основатель сохранял долю в компании после сделки. Как правило, покупатель даже в случае приобретения миноритарной доли (до 25%) хочет иметь возможность не просто наблюдать за деятельностью компании, но и существенным образом ее контролировать за счет согласования обширного перечня reserved matters, введения штрафных опционов на случай несогласованного поведения основателя и т. д. В то же время продавцы, если они остаются в компании, зачастую хотят продолжать действовать «как раньше» и не предоставлять инвесторам больше прав, чем предусмотрено приобретаемой ими долей;
3. **Сохранение команды**. Поскольку технологический бизнес сильно зависит от команды, одним из ключевых условий сделки становится удержание ключевых специалистов при вхождении нового или полной смене собственника компании. Здесь, как правило, возникают сложности для покупателя в выборе адекватных удерживающих механизмов с учетом свободы труда и невозможности заставить работника проработать в данной компании определенное время. Условия сопровождаемых нами сделок также предусматривали довольно серьезные последствия для продавца в случае «досрочного» ухода ключевых сотрудников вплоть до штрафных опционов с повышенной доходностью.



Александр Шалаев

партнер корпоративной практики

ELWI

Наиболее сложные вопросы, с которыми мы столкнулись при структурировании и согласовании сделок Tech M&A в 2025 г., были тесно связаны с очевидно несовпадающими коммерческими позициями сторон.

Разрыв в оценке таргета по-прежнему является ключевым переговорным вопросом и при согласовании сделок Tech M&A. Данный вопрос является очень «острым» и в сфере Tech M&A, поскольку активы таргета, как правило, достаточно сложно оценить. Одним из ключевых факторов, влияющих на цену таргета, становится видение перспектив роста бизнеса таргета или синергетического эффекта от встраивания таргета в бизнес покупателя. Продавец традиционно смотрит на перспективы оптимистично, в то время как со стороны покупателя оценка зачастую бывает более консервативной. Частично эти разногласия удается преодолеть с помощью механизма earn-out, позволяющего привязать оценку актива к росту бизнеса после закрытия сделки.

Что касается непосредственно юридических вопросов, по нашему опыту, немало «копий было сломано» юристами сторон по следующим вопросам:

- порядок определения имущественных потерь в различных сценариях утраты таргетом прав на ключевое ПО, в том числе с учетом разности оценок сторон стоимости такого ПО для бизнеса таргета;
- «классические» вопросы ограничения ответственности продавца в рамках процедур по ведению споров и срокам заявления соответствующих требований к продавцу;
- согласование «штрафных» опционов за нарушение продавцом ключевых обязательств в сделках с положениями earn-out;
- методология и процедурные вопросы независимого подтверждения достижения показателей, необходимых для earn-out корректировок;
- вопросы перехода долей в ООО к наследникам и наследования по соглашениям о предоставлении опци-

онов с физическими лицами (в случае невозможности предварительной реструктуризации владения долями / акциями на стороне продавцов);

- распределение компетенций между органами управления таргета с учетом продолжения продавцом работы в качестве генерального директора и сохранения доли участия продавца и наличия earn-out механизма (с учетом влияния покупателя / инвестора на принятие решений менеджментом).



Владислав Лазуткин

старший юрист

ORION

К специфическим факторам, оказывающим влияние на переговоры и структурирование Tech M&A сделок в 2025 г., можно отнести следующие:

1. Трансграничная фрагментация бизнеса таргета: единый целевой IT-бизнес может быть разделен на внешне независимые части: российскую, ориентированную на российских клиентов, и зарубежную часть, ориентированную на иностранных клиентов. Это усложняет due diligence, структуру сделки, расчетов, ключевых активов целевого бизнеса.
2. Ужесточение регулирования IT-бизнеса в РФ и за рубежом, тренд на локализацию чувствительных данных и технологий, повышение прозрачности операций и коммуникаций в интернете, формирование суверенного информационного пространства, а также урегулирование статуса игроков определенного сектора. Это требует больших ресурсов при осуществлении legal due diligence.
3. Санкционный контекст. Может оказывать влияние на структуры, используемые для сделки продавцом и покупателем (СФО, ЗПИФ, ДИТ и иные инструменты), и модель расчетов. Использование ряда структур, например ЗПИФ, требует учета связанной с ними специфики в части используемых инструментов в сделке (например, заверения об обстоятельствах, возмещение потерь, урегулирование ответственности УК и пайщиков).

Логика «рынка покупателя» изменила переговорный баланс при согласовании ценовых условий и подходов к распределению рисков в пользу риск-ориентированной позиции инвесторов.



Софья Смирнова

советник M&A
и корпоративной практики

O_2 консалтинг

По нашему опыту, самым острым вопросом в переговорах по юридическим аспектам создания совместных предприятий является вопрос о переходе долей к наследникам фаундеров (интересы обеих сторон понятны, но чаще всего в зависимости от многих факторов сделки и экономической ситуации, когда бизнесу необходимы деньги, а кредитование дорогое, фаундеры соглашаются, что их наследники получают компенсацию, не вступая в участники совместного предприятия). Иными краеугольными камнями переговоров, которые приходится фиксировать юридически, являются механизм ответственности продавца при нарушении обязательств в сделках с ценой earn-out (и пределы применения штрафных опционов), а также механизм расчета имущественных потерь при возникновении обстоятельств утраты прав на ключевое ПО (практику расчета по которым нельзя считать вполне сложившейся).

Усложнение процедур реструктуризации IT-активов

В ходе онлайн-опроса, проведенного в рамках исследования, участники сделок Tech M&A отметили, что **в 2025 г. существенно усложнились процессы, связанные с предпродажной реструктуризацией** IT-компаний и подготовкой таких активов к сделке.

#РЕЗУЛЬТАТЫ_ОПРОСОВ



Считают, что в 2025 г. усложнились процедуры предпродажной реструктуризации IT-компаний и «пересборки» периметра активов, а также отлагательные условия закрытия сделок



Считают, что при совершении сделок на поздних инвестиционных раундах или стратегических M&A стало сложнее «расшить» отношения с инвесторами предыдущих раундов

По данным Опроса по структурированию сделок Tech M&A в 2025 г.

Как показали итоги опросов, почти **треть респондентов** отметила, что в 2025 г. процесс подготовки IT-активов к продаже, а также **отлагательные условия закрытия Tech M&A сделок стали более сложными**. Часто в качестве такого условия стороны сделки предусматривали **завершение процедуры реструктуризации бизнеса** в соответствии с согласованным планом мероприятий.

Предпродажная реструктуризация бизнеса и процесс «пересборки» периметра ключевых активов является традиционным этапом Tech M&A-процесса. Помимо основной цели — **сформировать прозрачную целевую корпоративную структуру, на которой будут консолидированы ключевые активы бизнеса**, — этот процесс может включать другие более специфические задачи: (i) «расшивку»

отношений со структурами продавца, регулирование использования общих ресурсов или услуг на «переходный» период; (ii) решение вопросов брендирования продукта — разработку нового бренда или «выкуп» текущего; (iii) подготовку информационных систем и кодовой базы к процессу интеграции; (iv) выделение непрофильных или «токсичных» активов; (v) перестройку логистических цепочек; (vi) оптимизацию долговой и налоговой нагрузки.

Мы попросили ведущих юридических M&A-консультантов рассказать на примерах из своей практики об особенностях процесса предпродажной реструктуризации IT-компании в 2025 г.

#МНЕНИЕ_ЛИДЕРОВ_РЫНКА

Предпродажная реструктуризация в ИТ



Сергей Чапаев
партнер корпоративной практики

ELWI

Ситуации, в которых необходима предпродажная реструктуризация технологической компании, достаточно распространены. Причины могут быть разнообразными: например, стремительно развивающийся стартап достиг выдающихся результатов в короткие сроки, и его юридическое оформление просто не успевает за продуктовым. Нередко на начальном этапе сделки в таких компаниях еще нет четкой границы между «целевой компанией» и «группой продавца», и находить ее приходится непосредственно в процессе работы над сделкой. Существуют и обратные примеры, в которых взаимосвязи между целевой компанией и группой продавца (осуществляющей деятельность во многих юрисдикциях) формировались десятилетиями, что в итоге выливалось не только в привычную зависимость таргета от материнской группы, но и в более экзотическую ситуацию, в которой деятельность материнской группы значительным образом опиралась на услуги, предоставляемые таргетом. В результате одним из ключевых и наиболее сложных для согласования документов по сделке стал договор об оказании услуг на переходный период, в котором обе стороны, находящиеся в разных юрисдикциях, как оказывали, так и потребляли соответствующие услуги.

Для бизнесов с международным присутствием дополнительную сложность может вызывать необходимость координирования множества процессов по реструктуризации в нескольких юрисдикциях одновременно в целях приведения группы таргета в требуемое состояние к определенной дате, намеченной продавцом или обеими сторонами. В зависимости от изначальной и целевой точек работа может включать в себя как параллельные, так и последовательные треки, что требует тщательного планирования и тесного взаимодействия с одним или несколькими местными консультантами. Также необходимо убедиться, что положения ключевых лицензий и иных соглашений допускают такую реструктуризацию, либо заранее вступить в переговоры с контрагентами, чтобы избежать неприятных сюрпризов.

#РЕСТРУКТУРИЗАЦИЯ_IT_БИЗНЕСОВ



Софья Смирнова

советник M&A
и корпоративной практики

O_2 консалтинг

Предпродажная реструктуризация — часто встречающаяся в сделках ранних стадий процедура, которая отвечает сразу нескольким потребностям: 1) сформировать контур продажи, 2) митигировать наиболее значимые риски (в том числе стратегические), 3) сформировать комфортную оценку продаваемого бизнеса. Например, чаще всего с такой необходимостью сталкиваются фаундеры, которые смогли вывести продукт на определенный уровень выручки, но еще не привлекали стратегических инвесторов или имеют минимальный опыт работы с внешними структурами (в том числе финансовыми организациями). Часто встречается и потребность разделить российский и иностранный контуры, чтобы не смешивать инвесторов и продукты, рассчитанные на разную аудиторию. Наконец, подобная задача может встать от покупателя по итогам комплексной инвестиционной проверки (для избежания наследования определенных рисков новой структурой).

#РЕСТРУКТУРИЗАЦИЯ_IT_БИЗНЕСОВ



Анастасия Духина

старший юрист практики
корпоративного права / M&A

sll
SL LEGAL

В нашей практике было несколько сделок, предполагавших предпродажную подготовку актива. В одном случае она заключалась прежде всего в корпоративной реструктуризации группы компаний для создания прозрачной и управляемой структуры владения перед передачей ее приобретателю. В нескольких других случаях предпродажная подготовка предполагала переоформление IP&IT активов таргета. Так, в одной из недавних сделок требовалось передать права на интеллектуальную собственность в таргет от основателя или подконтрольных ему компаний, не вошедших в периметр сделки, а также разделить ИТ-инфраструктуру с зарубежным контуром таким образом, чтобы таргет мог бесперебойно продолжать свою деятельность. Сложность таких реструктуризаций заключалась в необходимости учесть особенности регулирования IT&IP вопросов в иностранных юрисдикциях, особенно если речь идет про недружественные страны и возможный санкционный элемент.

В другом случае существенный дискомфорт для покупателя представляло оформление прав на один из ключевых IP-активов не на компанию-таргет, а на ее участника, а также наличие различных взаимных обязательств между приобретаемой компанией и основателем, и требовалось включить в документы по сделке предварительные условия по переоформлению или реструктуризации «проблемных» отношений, невыполнение которых давало инвестору право отказаться от сделки.

#РЕСТРУКТУРИЗАЦИЯ_IT_БИЗНЕСОВ



Владислав Абрамов

директор по правовым вопросам

KAMA FLOW

Приходилось делать предпродажную реструктуризацию. Наиболее сложным в этом процессе была выработка оптимального сценария структурирования для соблюдения интересов всех сторон. Внутри группы активы зачастую бывают распределены между несколькими юридическими лицами, и требуется обеспечить, с одной стороны, юридическую прозрачность, а с другой — минимизацию рисков при переводе активов, включая нематериальные, на единый контур.

#РЕСТРУКТУРИЗАЦИЯ_IT_БИЗНЕСОВ



Байрас Магадеев

старший юрист
корпоративной практики

ELWI

В рамках сделки по приобретению клиентом доли в уставном капитале российской компании, занимающейся разработкой, производством, реализацией и обслуживанием автоматизированных депозитных машин, мы столкнулись со следующей особенностью: к моменту вхождения клиента в состав акционеров таргета часть акций уже была приобретена институциональным инвестором у основателя таргета. В связи с этим при обсуждении условий сделки необходимо было учитывать ранее достигнутые договоренности между основателем и институциональным инвестором, чтобы совместить их с коммерческой позицией клиента.

Как отмечает большинство Tech M&A-экспертов, характер и объем мероприятий по реструктуризации может быть весьма разнообразным и зависит от множества факторов.

В большинстве сделок с продуктовыми IT-активами важным этапом подготовки бизнеса к продаже является реализация мероприятий, направленных на восстановление прав в отношении ключевого ПО и других ОИС. Это обусловлено тем, что нередко существенная часть значимых активов IT-компаний к моменту сделки оказывается **«распыленной» среди широкого круга лиц, большая часть из которых находится за пределами контура владения компании**.

Например, права на различные ОИС в составе продукта, заявленного в маркетинговых материалах как «собственная разработка», одновременно могут принадлежать авторам-работникам компании, ее аффилированным структурам, в том числе «техническим», не входящим в периметр сделки, компаниям из группы продавца, их работникам и подрядчикам.

Проблема заключается в том, что такая «децентрализованная» структура владения **не создавалась целенаправленно и до проведения due diligence владельцы компании не видят «полной картины»**. Часто для самой компании такая ситуация оказывается «неприятным сюрпризом», несмотря на то, что основной ее причиной является невысокое качество оформления документации с разработчиками продукта. Поэтому до сделки компаниям часто **приходится «пересобирать» права на продукт и консолидировать управление и контроль над ними на единой структуре**. В 2025 г. наблюдался отчетливый тренд на хронологический сдвиг таких процессов «влево» относительно закрытия сделки. Этого требовал риск-ориентированный подход, применяемый большинством инвесторов в последнее время.

> **В продуктовых IT-компаниях существенная часть ключевых активов к моменту сделки нередко оказывается «распыленной» среди широкого круга лиц за пределами контура сделки. Поэтому покупатели требуют максимального устранения этих недостатков и передачи активов под контроль приобретаемой структуры. В 2025 г. этим процессам стало уделяться особое внимание в связи с более осторожным отношением инвесторов к риску.**

Однако комплекс мероприятий, проводимых в рамках подготовки IT-бизнесов к продаже, может быть значительно шире. Если компания относится к **определенному подсегменту IT-индустрии**, например, к сфере телекома, или имеет **присутствие в различных юрисдикциях**, например, является оператором глобальной ecommerce-платформы, — задачи, связанные с подготовкой актива к сделке, могут быть существенно сложнее. В таких случаях может потребоваться выделение отчуждаемого актива в самостоятельную корпоративную структуру и «очистка» периметра от элементов, связанных с остальной частью бизнеса.

Серьезным фактором, осложняющим процесс реструктуризации, является наличие в бизнесе «недружественного» иностранного элемента, от которого может зависеть оценка и функционирование его российской части, например, при использовании ею ресурсов международной группы. В таких случаях особой проработки требуют вопросы санкционного регулирования, оптимизации логистических цепочек, возможности замены услуг международных провайдеров, создания альтернативной договорной обвязки, разделения инфраструктуры, оценки последствий прекращения отношений с частью клиентской базы и поставщиками.

#РЕСТРУКТУРИЗАЦИЯ_IT_БИЗНЕСОВ



Александр Монин

партнер практики корпоративного права / слияний и поглощений

Melling Voitishkin &Partners

В сделках Tech M&A за 2025 г. мы проводили предпродажную реструктуризацию и консолидацию ключевых активов на таргете.

В области связи реструктуризация является неотъемлемой частью подготовки к сделке. Для того чтобы передать жизнеспособный бизнес в сфере телекома, его необходимо выделить в автономную, самостоятельную единицу, в том числе с точки зрения инфраструктуры. Дополнительная сложность заключается в том, что если компания является частью международной группы, то ее клиентская база зачастую является общей и для российского бизнеса. Соответственно, в ходе или после сделки российская дочерняя компания может потерять этих клиентов в связи с расторжением внутригрупповых договоров. Оказание ряда критических услуг в России после закрытия тоже может оказаться под вопросом ввиду прекращения доступа к глобальной инфраструктуре.

В области IT / software реструктуризации могут быть проведены в более ограниченном объеме: так, в одной из сделок нами была просто осуществлена единичная передача товарных знаков и доменных имен, которые были зарегистрированы на основателях бизнеса.

Необходимость дополнительных мероприятий, направленных на изменение текущей корпоративной структуры бизнеса, может быть обусловлена **особенностями формата основной сделки**. Например, при проведении редомициляции зарубежной компании в Россию может потребоваться предварительная реструктуризация ее структуры капитала. Зачастую холдинговая компания имеет сложную корпоративную обвязку между акционерами и компанией. Чтобы адаптировать такую структуру договоренностей к требованиям российского законодательства, может быть необходима предварительная корпоративная реструктуризация на уровне акционерного капитала иностранной компании.

#РЕСТРУКТУРИЗАЦИЯ_IT_БИЗНЕСОВ



Константин Саврыга

юрист

NIKOLSKAYA consulting

Отдельную сложность представляет адаптация корпоративной структуры и прав акционеров при переезде холдинговой компании в РФ. Классическая структура акционерного капитала зарубежных холдинговых компаний предполагает наличие нескольких классов акций, каждый из которых привязан к определенному раунду финансирования и имеет разный набор прав, включая конвертационную и ликвидационную квоты. Для стандартизации корпоративного управления и реализации прав акционеров-владельцев разных классов акций такие права осуществляются на as converted basis (при полной конвертации), fully diluted basis (при полном размытии) или as converted basis and on a fully diluted basis (сочетание обоих подходов).

Однако после 2022 г. многие инвесторы, структурировавшие приобретение акций через договоры конвертируемого займа в иностранные холдинговые компании, столкнулись с необходимостью получения российских регуляторных одобрений на конвертацию.

Одним из выходов из такого регуляторного тупика является контролируемая редомициляция холдинговой компании в РФ, однако российское законодательство, несмотря на гибкость, предоставленную Законом «О международных компаниях», все еще не позволяет полноценно реплицировать классические многоуровневые акционерные структуры. Более того, даже в пределах, допускаемых законодательством, могут возникнуть сложности при согласовании условий о выпуске акций с Банком России. А если стороны планируют осуществить событие ликвидности через IPO, то они вынуждены редомицилироваться в форме акционерного общества.

В таком случае стороны проводят предварительную реструктуризацию всего акционерного капитала, «уплощая» его до 1-го класса обыкновенных акций с одинаковыми правами. Такая реструктуризация требует не просто математического пересчета всех акций и прав к единому знаменателю, но и расшивки ряда прав определенных классов акций. Так как акции одного выпуска должны обладать идентичными правами, то часть прав

(в особенности специальные права якорных инвесторов, права со специальными пороговыми значениями, водопады дивидендных выплат и т. д.) должны быть отражены в корпоративном договоре в качестве личных прав конкретных акционеров, что, в свою очередь, требует разработки специальной механики передачи / ограничения передачи таких личных прав при отчуждении акций (как если бы отчуждались акции с такими правами).

#РЕСТРУКТУРИЗАЦИЯ_IT_БИЗНЕСОВ



Владислав Лазуткин

старший юрист

ORION

Предпродажная реструктуризация встречалась практически в каждой сделке и была осложнена, например, фактором трансграничной фрагментации бизнеса таргета, которая требовала сохранения того или иного актива за операционной компанией. В связи с этим прямолинейная консолидация была не всегда эффективна — требовался комплексный механизм, который также включает цепочку договорных связей компаний группы и инструменты владения долями в их капитале.

Кроме того, замена холдинга в одном из кейсов потребовала переноса структуры владения и конвертируемых в доли / акции инструментов на уровень новой головной компании группы таргета.

В 2025 г. по мере снижения риск-аппетита инвесторов процессы подготовки IT-активов к продаже стали ожидаемо более длительными и сложными. Инвесторы стремились войти в максимально очищенную от рисков структуру, понятную и прозрачную с точки зрения владения ключевыми активами и процессов корпоративного управления. Во многих IT-бизнесах текущий формат владения активами часто не соответствует требованиям инвестора к целевой структуре. Корпоративные реструктуризации, направленные на устранение этого разрыва, часто являются неотъемлемым этапом сделок в сегменте tech.

При проведении реструктуризации IT-компании важное значение приобретает оценка **налоговых последствий** для всех участников сделки, включая приобретаемую компанию, — в части сохранения ею налоговых льгот после завершения соответствующих мероприятий. Это актуально для любых форматов сделок Tech M&A, но особенно чувствительными налоговые последствия могут оказаться в проектах, совершаемых по **модели asset-deal**.

#РЕСТРУКТУРИЗАЦИЯ_IT_БИЗНЕСОВ



Антон Джуплин

партнер

АЛРУД

> В 2025 г. АЛРУД проводил такие реструктуризации и консолидации в российском контуре без участия зарубежных игроков. До 2025 г. АЛРУД сопровождал предпродажные реструктуризации в сделках Tech M&A с участием зарубежных игроков.

Консолидация активов и предпродажная реструктуризация могут подсветить исторические налоговые риски бизнеса. Основная сложность данного процесса заключается в том, как провести такие изменения с минимальными налоговыми рисками для продавцов (особенно физических лиц) и без переоценки стоимости бизнеса.

Так, одним из наиболее важных для технологического бизнеса аспектов является возможность сохранения налоговых льгот для ИТ-компаний по итогам реструктуризации. И в этом контексте необходимо учитывать ограничение на применение ИТ-льгот для некоторых компаний, участвовавших в корпоративной реструктуризации, что установлено абз. 19–21 п. 1.15 ст. 284 НК РФ, абз. 19–21 п. 5 ст. 427 НК РФ.

Некоторые клиенты используют альтернативу реструктуризации в связи с указанными ограничениями. В некоторых случаях также рассматривают возможность применения амнистии при дроблении бизнеса, установленной ст. 6 Федерального закона от 12.07.2024 № 176-ФЗ.

Помимо налоговых вопросов, могут возникать риски корпоративных конфликтов, когда среди участников есть основатели, отошедшие (самостоятельно или принудительно) от операционной деятельности. В таком случае каждое корпоративное действие необходимо верифицировать на предмет возможных корпоративных споров.

#РЕСТРУКТУРИЗАЦИЯ_IT_БИЗНЕСОВ



Сергей Еремин

партнер



Екатерина Борябина

юрист

NIKOLSKAYA consulting

Предпродажная реструктуризация IT-бизнеса в рамках asset-deal, связанной с передачей ПО и переводом персонала, требует тщательной оценки налоговых рисков.

В отличие от обычных для типовых asset-deal проблем с оценкой имущества для целей НДС, в сделках с IT-компаниями (где продаваемых основных средств либо нет вовсе, либо они несоразмерно дешевле профильных активов) на первый план выходит IT-льгота, утрата права на которую может иметь заметные последствия для бизнеса. Одним из требований для сохранения IT-льготы является наличие аккредитации, которая в том числе завязана на уровень заработной платы сотрудников, который должен быть не ниже среднего по РФ или соответствующему региону. При этом при характерном для asset-deal фактическом переводе сотрудников из одной компании в другую предыдущий работодатель квалифицированного персонала остается частично или полностью без работников, а значит, рискует не выполнить требование по заработной плате. Примечательно, что, хотя в законе отсутствуют требования о поддержании определенного количества сотрудников в штате, Минцифры обращает на это внимание при проверке наличия оснований для аккредитации.

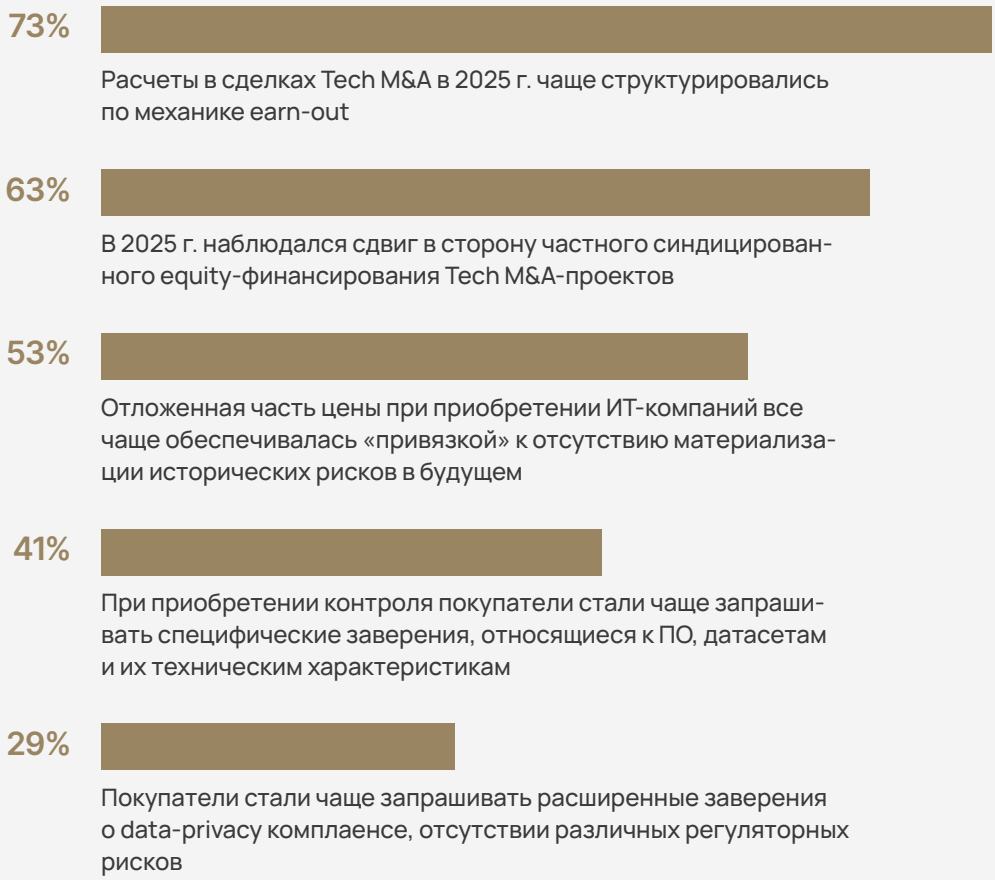
Другим налоговым аспектом при реструктуризациях выступает оценка возможности компании в случае утраты права на одни стимулирующие льготы претендовать на другие льготы, предусмотренные для IT-отрасли. Этот вопрос требует отдельного изучения в каждом конкретном случае.

3.2 Особенности структурирования сделок с технологическими активами в 2025 г.

В ходе онлайн-опросов мы попросили респондентов отметить наиболее значимые особенности сопровождения сделок с технологическими активами, которые они наблюдали в 2025 г. в своей практике.

#РЕЗУЛЬТАТЫ_ОПРОСОВ

Использование юридических механик и инструментов в сделках Tech M&A 2025



26%



В качестве основного инструмента распределения рисков чаще использовалась прямая корректировка цены

21%



Приобретатели ИТ-компаний для целей интеграции чаще проводили техническую экспертизу кодовой базы

11%



Инвесторы охотнее соглашались на расширение программ мотивации менеджмента при наличии качественной перспективны команды

9%



По нашему мнению, эти особенности были характерны для Tech M&A сделок всегда, не только в 2025 г.

По данным Опроса по структурированию сделок Tech M&A в 2025 г. (125 респондентов).



Артур Шубаев

партнер и исполнительный директор

ADVANCE CAPITAL

С точки зрения сопровождения сделок Tech M&A одной из ключевых сложностей является необходимость увязать юридическую конструкцию сделки с реальной бизнес-логикой технологического актива. В классических M&A-сделках основной фокус часто сосредоточен на правах на доли, финансовых обязательствах, материальных активах, трудовых отношениях и ключевых договорах. В Tech M&A к этому добавляется отдельный слой специфических вопросов: права на ПО и данные, open source компоненты, персональные данные, кибербезопасность, регуляторные ограничения, ИТ-льготы и др.

На sell-side одной из наиболее частых проблем является недостаточная готовность компании к due diligence. У быстрорастущих ИТ-компаний юридическая документация нередко отстает от фактического развития бизнеса: продукт уже масштабируется, клиенты подключены, команда расширяется, но права на отдельные элементы кода, отношения с подрядчиками, структура владения IP или порядок использования данных могут быть оформлены не в полном объеме. В результате вопросы, которые на ранней стадии воспринимались как технические или операционные, в сделке начинают напрямую влиять на оценку, сроки и перечень отлагательных условий.

Отдельный блок сложностей связан с удержанием команды и балансом интересов между инвестором и основателями. В технологических компаниях стоимость часто концентрируется не только в продукте, но и в людях, которые его создают. Поэтому юридическая документация должна не просто закрывать риски прошлого, но и создавать условия для устойчивого развития после сделки: через earn-out, опционы, KPI, ограничения на выход ключевых лиц, non-compete / non-solicit механики и понятную модель корпоративного управления.



Кристина Мкртчян

советник практики интеллектуальной собственности

ЭБР
Юридическая Компания

В 2025 г. усилилась тенденция к условному и риск-ориентированному ценообразованию: 73% респондентов указали, что расчеты чаще структурировались через earn-out.

Это показывает специфику технологических активов: покупатель не готов платить полную цену upfront, потому что бОльшая часть стоимости таргета зависит от будущих метрик: выручки, удержания команды, успешной интеграции продукта, подтверждения технологической работоспособности и отсутствия материализации IP / data / privacy-рисков.

63% респондентов отметили, что из-за отсутствия достаточной залоговой массы в ИТ-компаниях основными источниками финансирования остаются cash-in и акционерные займы, при этом наблюдается сдвиг в сторону синдицированного частного equity-финансирования.

Это можно объяснить тем, что у технологических компаний ключевые активы часто нематериальны, сложно оцениваемы и не всегда пригодны для классического залога. Поэтому финансирование строится вокруг equity-логики и доверия к будущему росту, а не вокруг обеспеченного долгового инструмента.

53% респондентов указали на «привязку» части платежа к отсутствию материализации рисков как на основной способ обеспечения финансовых обязательств таргета. Это фактически заменяет классическое обеспечение более гибким механизмом удержания части цены или отложенного платежа, завязанного на качество раскрытия, отсутствие претензий и устойчивость технологического актива после закрытия сделки.

Как показали результаты опроса, в 2025 г. ключевыми транзакционными механиками, обеспечивающими гибкость в структурировании договоренностей сторон и балансировку разнонаправленных интересов, являлись **earn-out** (**73% респондентов**), **синдицированный cash-in** (**63% респондентов**) **и holdback** (**53% респондентов**).

Мы попросили Tech M&A-экспертов рассказать о наиболее интересных аспектах структурирования этих юридических механик.

3.2.1 Механика earn-out

Механика earn-out позволяет сторонам, инвестиционные кейсы которых критически расходятся, договориться о сделке «сегодня» и предусмотреть гибкий механизм перерасчета цены при достижении бизнесом согласованных КПЭ в будущем. В сделках Tech M&A механика earn-out наиболее распространена, поскольку это обусловлено спецификой IT-сектора. Даже в устойчивых макроэкономических и конъюнктурных условиях бывает **крайне сложно оценить стоимость развивающегося бизнеса, в основе которого лежат нематериальные активы, и динамику поведения его ключевых операционных метрик**. В 2025 г. ориентиры оценки IT-компаний оказались еще более размытыми, поэтому earn-out использовался практически во всех сделках с технологическими активами.

При использовании механики earn-out покупатель на закрытии сделки выплачивает продавцу «понятную» ему часть цены, соответствующую его взгляду на текущую оценку бизнеса (EV). Если продавец считает, что актив стоит дороже, но не может обосновать более высокую оценку на момент входа в сделку, — он получает возможность «дозаработать» дополнительную стоимость и получить в будущем дополнительную часть цены. Earn-out работает «вправо» относительно базовой цены и **направлен на обеспечение роста стоимости бизнеса (EV) и / или повышение его эффективности**. Его выплата «авансом», рассчитанным на основе кейса продавца, не соответствует сложившейся бизнес-практике применения этой механики, создает дополнительные риски для покупателя, связанные с необходимостью обеспечения возврата цены в случае реализации негативного сценария, и не применима в условиях «рынка покупателя».

#МНЕНИЕ_ЛИДЕРОВ_РЫНКА

Сначала докажи!



Мария Баева
партнер, корпоративная практика,
глава коммерческой практики

Использование механики ценообразования earn-out становится все более распространенным явлением в сделках Tech M&A. В этом отношении 2025 г. не выбивается из общего тренда. Основная причина роста популярности инструмента — большое количество сделок по поглощению крупными IT-компаниями небольших и средних по размеру стартапов, владельцы которых зачастую не имеют сильных переговорных позиций. В такой ситуации earn-out выступает в качестве компромиссного сценария, в рамках которого IT-гигант получает перспективный стартап относительно недорого «здесь и сейчас», а продавцы-основатели оставляют за собой возможность получить оплату в большем размере, если таргет оправдает свою перспективность под «крылом» нового собственника. Что касается периодов earn-out, то в наших кейсах в рамках Tech M&A они редко составляют более двух лет: чаще всего это либо единственный платеж по итогам года, либо разбитый на несколько частей платеж, выплачиваемый в течение двух лет.

В наших сделках мы видели самые разные KPI, обусловливающие отложенный платеж и его размер. Наиболее часто встречающиеся варианты: пороговые значения выручки за определенный период, таргеты по маржинальности бизнеса, обеспечение выполнения мероприятий по интеграции сервисов и продуктов стартапа в сервисную и продуктовую линейку покупателя, обеспечение удержания ключевого IT-персонала.

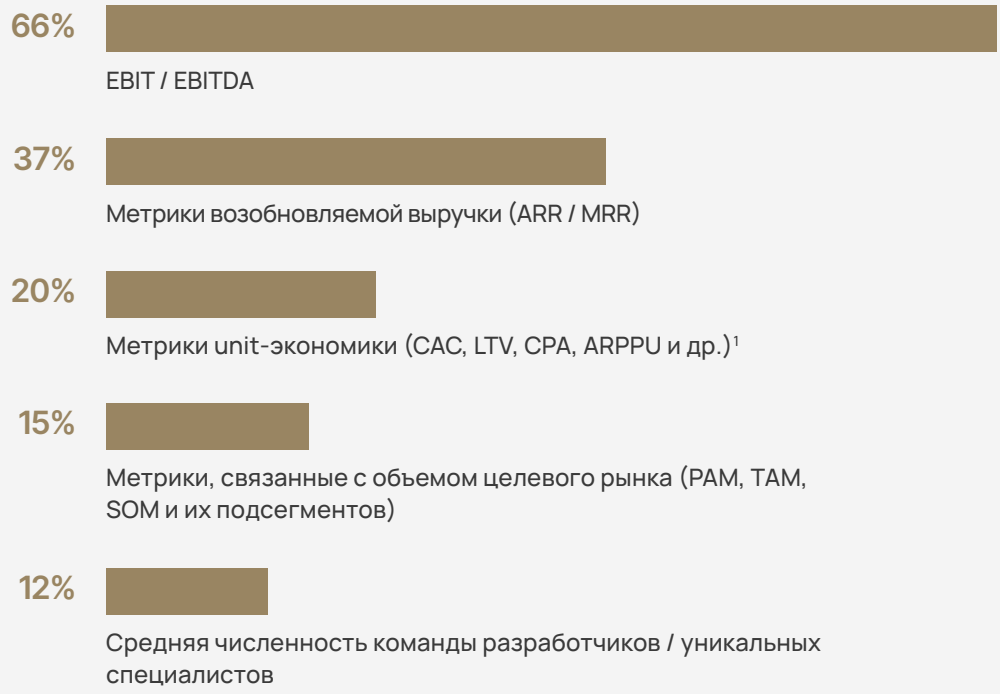
Наиболее сложный аспект структурирования earn-out — это обеспечение его сбалансированности: выгода от достижения KPI должна возникать у обеих сторон, что существенно снижает риски злоупотреблений «на пути» к выполнению KPI. Также бывает непросто выстроить действительно эффективную систему «сдержек и противовесов», призванную отсекать недобросовестное поведение той или иный стороны.

По крайней мере в одной из наших сделок в 2025 г. мы использовали комбинацию earn-out с опционными механизмами, в рамках которой у основателя оставалась миноритарная доля, которая была выкуплена покупателем по колл-опциону после достижении KPI. В данном случае риски основателя были митигированы тем, что опцион был двусторонним: если бы покупатель не реализовал колл-опцион, основатель смог бы воспользоваться предоставленным ему пут-опционом.

С юридической точки зрения earn-out является **разновидностью отложенного обусловленного платежа, при котором его размер изначально не известен**, но может быть определим в зависимости от согласованных сторонами параметров. В отличие от более широкой модели обусловленного отложенного платежа, размер которого может быть известен заранее, механика earn-out направлена преимущественно **на обеспечение прироста стоимости бизнеса (EV) или увеличение его эффективности и, соответственно, определение размера итоговой цены**. При этом КПЭ, выполнением которых обусловлена выплата дополнительной части цены, должны обеспечивать сторонам, и прежде всего покупателю, возможность обоснования прироста стоимости.

#РЕЗУЛЬТАТЫ_ОПРОСОВ

Какие метрики лежали в основе earn-out в известных вам сделках Tech M&A в 2024–2025 гг.?



По данным Опроса по аспектам Tech M&A (41 респондент).

[1] См. детализацию метрик unit-экономики в приложении 1.

Как показали результаты опроса, проводимого в отношении сделок Tech M&A преимущественно mid-market сегмента 2024–2025 гг., механика earn-out чаще всего основывалась на финансовых метриках EBIT / EBITDA и возобновляемой выручки (ARR, MRR). В 2025 г. в процессе определения стоимости и оценки общего качества бизнеса стали чаще использоваться метрики unit-экономики. Однако их более низкая популярность (отметили всего **20% респондентов**) при структурировании модели earn-out в сравнении с финансовыми метриками объясняется тем, что КПЭ, основанные на unit-экономике, крайне сложны для фиксации, мониторинга и верификации. В сделках с участием стратегических покупателей earn-out может быть «привязан» к метрикам, связанным с реализацией синергий, например, параметрам, определяющим число пользователей продукта компании, которые после закрытия сделки получили доступ к комплементарным продуктам приобретателя.

#EARN-OUT



Федор Муходанов

старший юрист практики корпоративного права / слияний и поглощений

Melling Voitishkin &Partners

> KPI, к которым был привязан дополнительный платеж в рамках earn-out:

1. Выручка таргета.
2. Бизнес-параметр (успешная миграция определенного числа пользователей онлайн-платформы таргета на платформу покупателя).

Срок выплаты дополнительного платежа в рамках earn-out: один год с даты подписания договора купли-продажи.

Основная сложность заключалась в структурировании бизнес-параметра. Процесс миграции потребовал детальной проработки IT-специалистами перед его согласованием сторонами, поскольку являлся технически сложным и зависел от множества факторов (например, каким образом пользователи изначально проходили регистрацию и оплачивали подписку).

Другой сложной задачей стала разработка процедуры верификации выполнения KPI, в частности определение того, кто и каким образом подтверждает корректность расчета успешно мигрировавших пользователей. Для итогового подтверждения выполнения KPI стороны согласовали специальный документ — двусторонний акт выполнения KPI, который подписывался обеими сторонами, а также процедуру согласования акта в случае отказа одной из сторон подписать указанный акт.

#EARN-OUT



Анастасия Духина

старший юрист практики корпоративного права / M&A

sll
SL LEGAL

За последний год в наших сделках earn-out редко делился более, чем на 2 этапа. Как правило, часть покупной цены платилась на этапе закрытия или около него (и согласование размера и момента оплаты на этом этапе было едва ли не одним из самых сложных вопросов в переговорах), а вторая часть выплачивалась через год с возможностью ее корректировки в зависимости от достигнутых компанией показателей по EBITDA, выручке и чистому долгу (в любых сочетаниях).

#EARN-OUT



Тигран Микаелян

юрист корпоративной практики

ELWI

По нашему опыту, в 2025 г. механика ценообразования earn-out была привязана к достижению таргетом таких показателей, как выручка и EBITDA, а также к увеличению рыночной стоимости долей по независимой оценке. Период earn-out, как правило, составлял от двух до четырех лет. В качестве механизмов структурирования earn-out платежей в сделках мы встречали:

- корректировку покупной цены в рамках договора купли-продажи, по которому покупатель приобретал первоначальную долю в таргете;
- опцион по дальнейшей консолидации инвестором 100% в таргете, цена по которому привязана к достижению таргетом определенных показателей (выручка, EBITDA);
- опцион по дальнейшей консолидации инвестором 100% в таргете, цена по которому определялась независимым оценщиком;
- комбинация вышеперечисленных опций.

Большинство Tech M&A-экспертов отметили, что в сделках 2025 г. earn-out период в среднем не превышал двух лет, структура платежа включала обычно два транша, а в качестве элемента договорной обвязки все чаще использовались опционы.

Если дополнительный платеж был обусловлен метриками, которые сами по себе **не являлись драйвером стоимости бизнеса и не позволяли определить прирост EV**, по окончании периода earn-out стороны проводили повторную оценку и определяли разницу с первичной. Новая оценка могла осуществляться силами стороннего эксперта, привлекаемого в соответствии с заранее согласованной процедурой. Однако такой подход является менее прозрачным. При использовании КПЭ, влияние которых на рост бизнеса неявно, прирост его стоимости или увеличение эффективности могли быть вызваны другими факторами, не связанными с выполнением КПЭ, действиями продавца или компании.

В российской бизнес-практике устоялся подход, при котором в модели earn-out в качестве КПЭ используются совершенно разные условия и факторы, в том числе не имеющие прямого влияния на рост стоимости бизнеса. Основными из таких КПЭ, косвенно влияющих на динамику оценки, являются требование удержания команды после закрытия сделки, а также завершение процедур реструктуризации бизнеса, перевод контрактов, отдельных активов, регистрация нового бренда и т. п.

#EARN-OUT



Антон Джуплин

партнер

АЛРУД

Одна из сделок предполагала совершение предпродажной реструктуризации в виде перевода ключевых контрактов с компаний за периметром сделки на таргеты. Такая реструктуризация являлась отлагательным условием. Earn-out был привязан к определенной шкале процента перевода оборотов по таким контрактам: не более 65%, более 65% и менее 85%, более 85%, а также к достижению определенного показателя take-rate. Срок предполагался довольно короткий — 3 месяца с возможностью пролонгации на дополнительные 3 месяца. Наиболее сложным в переговорах было договориться о критериях реструктуризации, ее шагах и способе подтверждения условий по оборотам, если перевод контрактов в существенной степени зависел как от содействия самих контрагентов, так и от влияния покупателя на процесс в виде необходимости согласования условий с ним или подконтрольными ему контрагентами таргетов. Опционы в такой конструкции не использовались, при этом право продавца на выход из сделки было также ограничено.

В другой из сделок earn-out механизм был привязан к выручке и некоторым параметрам интеграции таргета в экосистему покупателя. Сложность переговоров по этим вопросам заключается в том, что продавцы часто не согласны с такими KPI, так как они не всегда могут повлиять на достижение этого KPI. Например, если для интеграции нужен дополнительные бюджет, то продавцы не могут повлиять на его выделение на уровне покупателя / таргета.

#EARN-OUT



Татьяна Кассирова

советник корпоративной практики

ELWI

Мы осуществляли полное юридическое сопровождение сделки на стороне покупателя по приобретению компании, предоставляющей аналитику по оценке эффективности маркетинга через блогеров. Для покупателя достаточно распространенным в сделках подобного рода является вопрос сохранения не только объектов интеллектуальной собственности, принадлежащих компании и являющихся существенным элементом ее деятельности, но и сохранения ключевого менеджмента — основателей бизнеса и создателей первоначальной идеи. Так, в данной сделке одним из наиболее важных аспектов было структурирование сделки таким образом, чтобы в течение определенного периода времени после закрытия основатели бизнеса продолжали работать в компании и передавали свои знания, опыт и понимание специфики компании покупателю. Данный вопрос был решен путем использования механизма earn-out в рамках структурирования оплаты покупной цены, который предполагает отложенные выплаты продавцам в течение определенного периода времени после закрытия при достижении компанией согласованных результатов. Это соответствует интересам покупателя, так как позволяет сохранить ключевых работников и дает возможность покупателю погрузиться в специфику бизнеса, обеспечивая при этом непрерывность управления бизнес-процессами. Для продавцов данный механизм также является интересным, так как позволяет получить дополнительный доход от деятельности компании даже после продажи бизнеса.

#EARN-OUT



Ксения Збышевская

советник

NIKOLSKAYA consulting

По нашему опыту, в технологических компаниях главными активами являются объекты интеллектуальной собственности и ключевые сотрудники. Без их перехода теряется коммерческая целесообразность сделки.

Складывается ситуация, при которой покупатель не готов платить до получения уверенности в передаче активов, а продавец не передаст их без гарантий оплаты. Чтобы сбалансировать риски сторон, покупная цена разбивается на транши, привязанные к наступлению конкретных условий, — рассмотрим на примере программного обеспечения:

- **Проверка работоспособности**. Покупателю важно убедиться в работоспособности кода, но такая проверка требует его раскрытия. Это риск для продавца, так как контрагент-конкурент может отказаться от сделки и скопировать технологию. Обычно покупатель не удовлетворяется гарантиями из заверений, а продавец — заключением NDA, поэтому такое раскрытие кода можно поставить под условие оплаты части покупной цены.
- **Переход ключевой команды**. Основная группа разработчиков, создавшая и поддерживающая ПО, должна перейти к покупателю — без них код теряет ценность. Продавец организует переход команды, но одновременно обеспокоен риском отказа покупателя от сделки. Соответственно, такой переход также может быть поставлен под условие уплаты части цены.

Выполнение условий часто подтверждает независимый консультант, что снижает риск предвзятости внутренних проверок.

#РЕЗУЛЬТАТЫ_ОПРОСОВ



Считают механизм earn-out с условием удержания команды наиболее эффективным средством от переманивания ключевых работников.



Считают, что лучшая мотивация команды обеспечивается через мотивацию продавца с использованием earn-out, который сможет премировать работников из «дозаработанной» цены.

По данным Опроса по структурированию сделок Tech M&A в 2025 г.

#EARN-OUT



Владислав Лазуткин

старший юрист

ORION

Основной инструмент удержания команды после закрытия сделки — earn-out в привязке к базовым показателям деятельности компании, от которых зависит ее оценка.

В случае многостадийного приобретения основными факторами мотивации являлись: (i) сохранение за командой доли в бизнесе и (ii) наличие опционов на приобретение стратегическим покупателем контроля над компанией с привязкой их условий к показателям деятельности компании на горизонте нескольких лет. В ряде случаев используется механизм ratchet — корректировки доли покупателя с учетом динамики бизнес-показателей.

#EARN-OUT



Анастасия Духина

старший юрист практики корпоративного права / M&A

sll

Помимо внедрения действенных мотивационных программ для сотрудников приобретаемой компании (включая долгосрочные программы мотивации с предоставлением акций или иным образом привязанные к росту стоимости компании), защитой от переманивания может быть (i) интеграция новой команды с командой приобретателя (защита от внезапной потери компетенции в связи с уходом «новых» сотрудников) и (ii) привязка этапов выплат по earn-out к сохранению команды (например, уход каждого ключевого сотрудника сокращает выплату по earn-out на X%), или сочетание этих инструментов. Однако в нашей практике далеко не все приобретатели готовы настолько детально регулировать вопросы удержания сотрудников и защиты от переманивания в документах по сделке.

В российской бизнес-практике в качестве основного или дополнительного КПЭ в модели earn-out широко распространено условие удержания ключевых работников после закрытия сделки в течение согласованного срока.

3.2.2 Расчетные корректировки цены

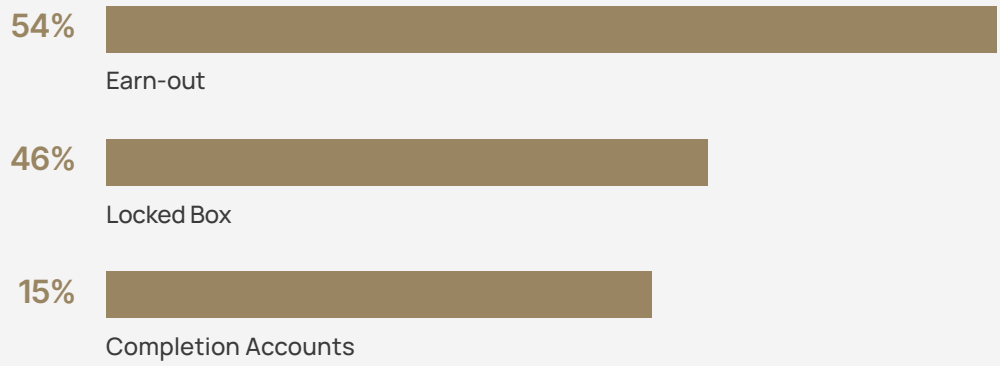
Механика earn-out определяет динамику **стоимости бизнеса (EV)** и прежде всего направлена на обеспечение ее роста. При расчете стоимости акционерного капитала (E) дополнительно определяется стоимость компонентов чистого долга и, если применимо, чистого оборотного капитала[2]. Приведение к согласованным параметрам при наличии фактических отклонений осуществляется с помощью механик locked box или completion accounts. Поэтому с механизмом earn-out в большинстве случаев дополнительно используется одна из указанных механик, фиксирующих переход к стоимости акционерного капитала, а иногда — их сочетание.

В рамках исследования мы провели онлайн-опрос, в котором попросили респондентов отметить, какие механики фиксации стоимости бизнеса и компонентов чистого долга они обычно используют в сделках Tech M&A. Опрос относился к периоду 2024–2025 гг., его результаты приведены ниже.

[2] Переход от величины EV к E осуществляется по формуле т. н. «EV-to-E bridge». Наиболее распространена краткая формула расчета стоимости акционерного капитала — E = EV − ND, где ND — показатель чистого долга.

#РЕЗУЛЬТАТЫ_ОПРОСОВ

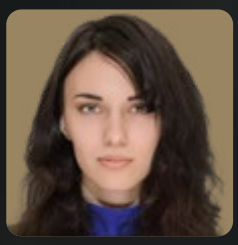
Какие механики завершения расчетов и оценки вы наиболее часто использовали в сделках Tech M&A?



По данным Опроса по аспектам Tech M&A (41 респондент).

Результаты опроса показали, что наряду с механикой earn-out, направленной на рост EV, наибольшей популярностью в сделках Tech M&A пользуется расчетная корректировочная механика locked box (**46% респондентов**). Существенно реже в сделках tech-сегмента используется механика completion accounts (**15% респондентов**). При этом в абсолютном большинстве случаев они сочетаются с механикой earn-out, если таковая используется в качестве базовой модели фиксации стоимости бизнеса.

#КОРРЕКТИРОВОЧНЫЕ_МЕХАНИКИ



Анастасия Нерчинская

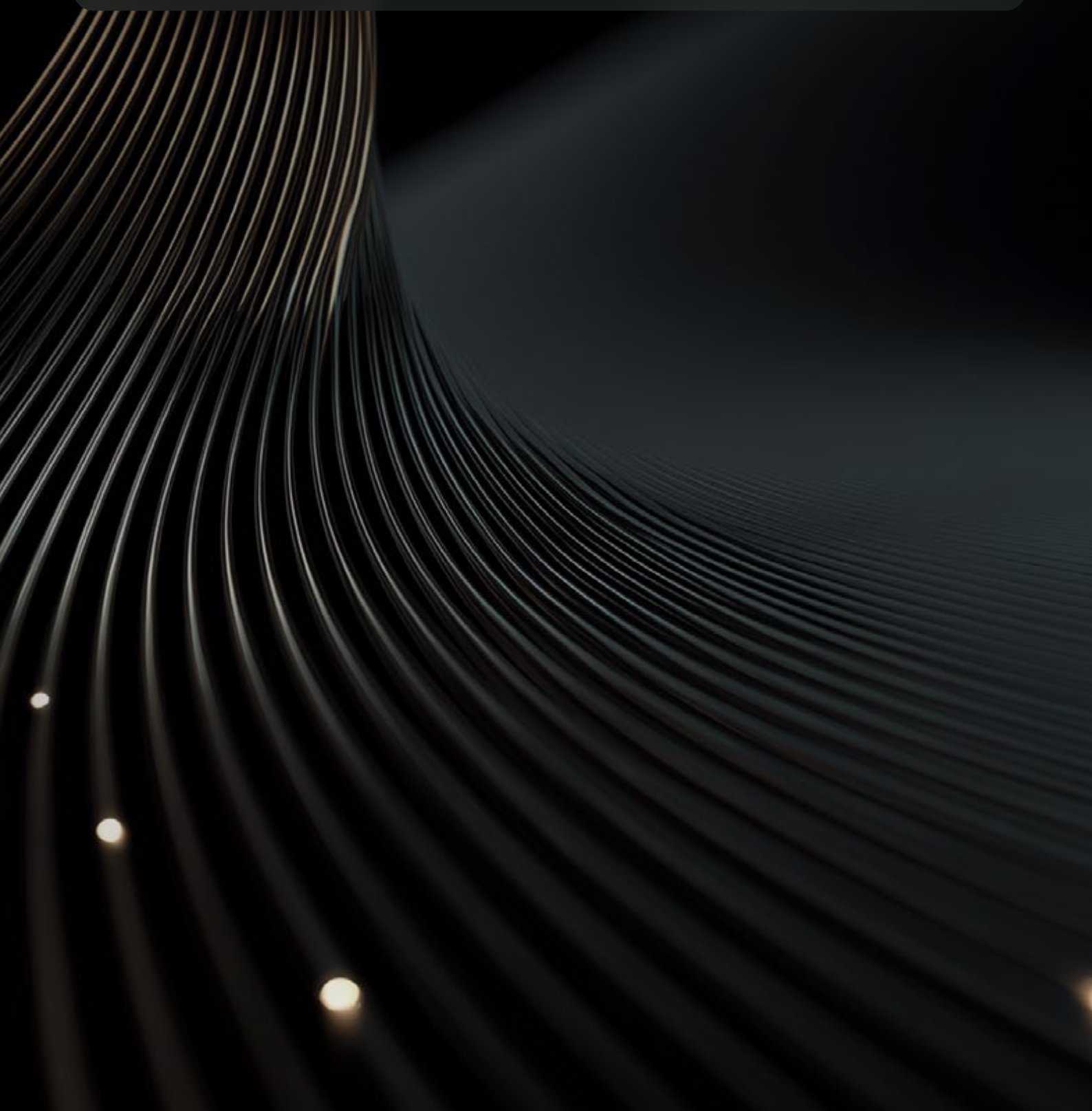
@SDELKIMNA →

M&A I AI →

Популярность механики locked box, фиксирующей изменение стоимости компонентов чистого долга и оборотного капитала по сравнению с их первоначально согласованной величиной, объясняется несколькими факторами. Во-первых, большинство сделок в tech относится к сегменту mid-market, а венчурные инвестиции — к low-market. Использование механики completion accounts, особенно в ее сочетании с earn-out, связано с очень высокими накладными расходами даже для сделки среднего ценового сегмента. Во-вторых, большинство сделок Tech M&A связано с продуктовыми активами, в которых уровень чистого долга традиционно не является высоким, в том числе по причине отсутствия банковских кредитов. В таких условиях использование механики completion accounts может быть неоправданно долго, дорого и малоэффективно. Покупатели понимают, что если у компании низкий уровень долга и свободных денежных средств, основной продукт представлен в форме нематериальных активов, а цена будет выплачена в пределах финансового года, проведение сложной и дорогостоящей процедуры completion accounts может быть излишним.

Иная ситуация имеет место в сделках Tech M&A сегмента high-market. К этому сектору рынка TMT относятся зрелые компании с высокой стоимостью бизнеса (EV), среди которых много капиталоемких и инфраструктурных проектов, где традиционно высоки рыночные барьеры входа. Компании этого сегмента производят не только цифровые продукты, но и электронные устройства и IT-оборудование. Стоимость компонентов чистого долга в таких активах может быть гораздо выше, поскольку, в отличие от софтверных компаний, они кредитуются банками и имеют более широкий доступ к заемному финансированию. Структура оборотного капитала многих таких компаний также более сложна. Она, помимо параметров дебиторской и кредиторской задолженности, часто включает компонент запасов, что требует тщательной сверки при закрытии расчетов.

В этих случаях использование процедуры completion accounts более оправдано, особенно в ситуации «рынка покупателя». В 2025 г. такая механика нередко встречалась в сделках сегмента high-market, позволяя покупателям лучше контролировать динамику изменений компонентов чистого долга и чистого оборотного капитала при осуществлении расчетов.



В сделках Tech M&A распространена практика использования **гибридных моделей**, сочетающих элементы locked box и competion accounts, в том числе в комбинации с earn-out, который является самостоятельным элементом. Механизм locked box позволяет сторонам применить **юридический механизм защиты от утечек**. В первую очередь эта цель достигается за счет инструментария обязательств продавца воздержаться от совершения определенных действий до закрытия сделки без согласования покупателя (pre-closing conduct), а также компенсационных механизмов на случай нарушения — например, возмещения имущественных потерь. Правовые средства в рамках применения механики completion accounts позволяют обеспечить **корректировку цены**, если, несмотря на механизм защиты от утечек, на дату закрытия сделки увеличилась стоимость компонентов чистого долга и оборотного капитала, по сравнению с ранее согласованной величиной.

На практике перечень поведенческих обязательств продавца бывает **существенно шире, чем те, что покрываются механикой locked box**, защищающей стоимость от утечек денежного характера. В стандартный перечень обязательств продавца до закрытия сделки принято включать и те, **что направлены на защиту от размытия** не только той части стоимости, что связана с компонентами чистого долга и неоперационными активами, **но и непосредственно стоимости бизнеса (EV)**. Наиболее важными из них являются запрет на совершение сделок с ключевыми активами, в первую очередь ПО, данными и инфраструктурой, без предварительного согласия покупателя, а также перепрофилирование бизнеса или иное его существенное изменение.

На выбор механики фиксации изменения величин чистого долга и оборотного капитала, используемой одновременно с моделью earn-out, влияет множество факторов. Один из них — период earn-out. Если он составляет продолжительный период, стороны чаще сочетают обе механики (что не обязательно), например, используют locked box в рамках первого транша, а completion accounts — при завершении расчетов.

#КОРРЕКТИРОВОЧНЫЕ_МЕХАНИКИ



Михаил Локтионов

партнер

STONEBRIDGE LEGAL

В 2025 г. при структурировании покупной цены в Share Deals в отношении ИТ-активов в нашей практике преобладали механизмы completion accounts, комбинированные с earn-outs или отсроченными платежами.

В рамках completion accounts стороны всегда предусматривали корректировку на чистый долг, а также, в зависимости от специфики бизнеса ИТ-актива, включали корректировку на оборотный капитал. Последняя применялась, как правило, в случаях, когда использование ИТ-актива было функционально связано с поставляемым физическим устройством или иным материальным компонентом, которые учитывались в составе оборотного капитала таргета; при этом корректировка покупной цены была связана с наличием таких устройств и компонентов на дату закрытия.

Приобретение ИТ-актива в большей мере, по сравнению с другими видами активов, связано со сложностями оценки его рыночной стоимости. В связи с этим для снижения риска несоответствия покупной цены и действительной стоимости ИТ-актива стороны в большинстве случаев предусматривали механизм earn-outs. В сопровождаемых сделках, структурированных таким образом, использовались два типа earn-outs: (i) нефинансовый earn-out, преимущественно привязанный к количеству пользователей ИТ-актива за определенный период после закрытия сделки, и (ii) финансовый earn-out, основанный на достижении показателей выручки от использования ИТ-актива. Размер earn-outs в сопровождаемых сделках составлял до 15% от базовой покупной цены.

На срок выполнения KPI, связанных с earn-outs, продавец-фаундер и его команда сохраняли позиции в таргете, обеспечивая выполнение KPI при контроле покупателя на операционном уровне и возможности проверки выполнения KPI через независимого аудитора.

В сделках в отношении ИТ-активов без использования earn-outs стороны согласовывали отложенный платеж, используемый покупателем, в том числе для обеспечения достоверности заверений и обязательств продавцов по возмещению имущественных потерь.

#КОРРЕКТИРОВОЧНЫЕ_МЕХАНИКИ



Федор Муходанов

старший юрист практики корпоративного права / слияний и поглощений

Melling Voitishkin &Partners

В одной из сделок при приобретении IT-бизнеса использовалась гибридная модель, предполагающая сочетание механизма locked box и completion accounts: фиксированная цена, установленная на определенную дату, подлежала корректировке на размер чистого долга и чистого оборотного капитала компании-таргета на дату закрытия сделки. Данная конструкция также включала корректировку покупной цены в пользу покупателя в случае возникновения утечек (locked box).

Таким образом, стороны отказались от механики locked box в ее классической форме в пользу гибридного подхода, который включал элементы корректировки по ключевым финансовым показателям таргета для учета изменений в периоде между датой, на которую согласована цена, и датой перехода контроля к покупателю.

В другой сделке ключевая цель механики completion accounts была достигнута не через корректировку цены после закрытия, а через институт возмещения потерь. В договоре были зафиксированы показатели чистого долга и оборотного капитала, а также установлен порог отклонения от данных показателей. Если фактические показатели ухудшались на сумму, превышающую этот порог, покупатель получал право заявить требование о возмещении потерь.

Важно отметить, что данная механика работала исключительно в пользу покупателя, поскольку не предусматривала доплаты продавцу в случае улучшения показателей, что отражало сильную переговорную позицию покупателя.

Одним из ключевых факторов, влияющих на выбор механики корректировки цены, является баланс переговорных сил сторон. В ситуации, когда превалирует позиция покупателя, стороны обычно склоняются к использованию механизма completion accounts, который традиционно считается более благоприятным для приобретающей стороны.

#КОРРЕКТИРОВОЧНЫЕ_МЕХАНИКИ



Анастасия Духина

старший юрист практики корпоративного права / M&A

sll
SL LEGAL

В сделках с использованием completion accounts данный механизм корректировки цены использовался как более прямолинейный и предсказуемый для обеих сторон и, соответственно, создающий более низкий риск спора о расчетах. При этом в одной из наших сделок стороны использовали комбинацию механизмов completion accounts и locked box для наиболее точной итоговой оценки приобретаемого бизнеса.

3.2.3 Механика holdback

Еще одной распространенной механикой структурирования сделок Tech M&A является т. н. удержание части цены или holdback. **53% респондентов** опроса, приведенного выше, отметили, что в 2025 г. в сделках Tech M&A чаще использовалась механика защиты покупателя от исторических рисков, реализуемая через удержание части цены (holdback). В отличие от механики earn-out, направленной на обеспечение прироста стоимости бизнеса, у модели holdback иное целеполагание — **обеспечить защиту покупателя от материализации уже имеющихся рисков**, стоимость которых была перераспределена на продавца с помощью договорных механизмов.

Отложенный платеж используется как самостоятельная механика в случаях, когда цена сделки уже известна на дату закрытия, то есть без использования earn-out, или вычитается из первого транша при использовании earn-out.

Как отмечают многие эксперты, в 2025 г. механика holdback стала использоваться чаще, что соответствует логике «рынка покупателя». Отложенный платеж, служащий страховкой от исторических рисков, является очень сильным защитным инструментом, который помимо компенсационной функции включает и обеспечительную. В 2025 г. с усилением внимания покупателей к рискам модель holdback чаще использовалась в сделках Tech M&A, особенно в случаях, когда продавцом выступало физическое лицо.

Покупатели настаивают на удержании части платежа без использования эскроу. Однако в сделках с качественными активами продавцы охотнее соглашаются на такую механику при резервировании страховочной суммы у третьей стороны с распределением расходов и контролем доходности на случай, если риски не материализуются.

#МНЕНИЕ_ЛИДЕРОВ_РЫНКА

Механизм уменьшения цены в сделках Tech M&A: наш опыт в 2025 г.



Александр Шалаев
партнер корпоративной практики

ELWI

Механизм уменьшения покупной цены является удобным и эффективным инструментом защиты прав покупателя, т. к. в случае выявления проблем с активом после закрытия сделки покупателю не требуется предварительно судиться с продавцом и взыскивать суммы убытков или имущественных потерь в рамках арбитражного разбирательства и далее в исполнительном производстве. Эти суммы попросту вычитаются из отложенного платежа покупателя.

За последний год в сделках Tech M&A, как и в классических M&A сделках мы редко встречали использование инструмента уменьшения покупной цены в качестве общего механизма защиты покупателя, если только речь не шла о сделке с участием физического лица — продавца, который не имел иных существенных активов, помимо продаваемых акций / доли. Как правило, уменьшение покупной цены имело место в сделках по продаже 100% в таргете и было связано с отложенным платежом части покупной цены, который обеспечивал:

- защиту покупателя от какого-либо реального риска (например, вероятных налоговых доначислений, идущего судебного спора) или
- погашение задолженности или прекращение поручительства какого-либо общества из периметра приобретаемой группы.

При этом редкость использования данного механизма объясняется, в первую очередь, тем, что продавцы не соглашаются с такими положениями и даже готовы «не идти в сделку», обосновывая это тем, что покупатель уже получил контроль и все права в отношении таргета (получил доступ к ПО, имеет право на получение дивидендов и т. д.). Согласование такого механизма требует сильной переговорной позиции на стороне покупателя.

Для иллюстрации: в нашей практике сделок Tech M&A в 2025 г. мы использовали механизм уменьшения цены в одной из многоэтапных сделок. По условиям сделки, требования покупателя в связи с недостоверностью заверений или наступлением обстоятельств возмещения потерь по договору в рамках первоначального «входа» покупателя в таргет уменьшали покупную цену продажи долей по опционам на последующих этапах консолидации покупателем 100% доли в таргете на сумму таких требований покупателя. При этом отметим, что в данном примере инструмент уменьшения покупной цены также использовался в обеспечительных целях для уменьшения риска отсутствия у продавца достаточных активов для удовлетворения требований покупателя.

С юридической точки зрения реализация механики holdback достаточно сложна. В ее базовом сценарии покупатель получает право уменьшить цену сделки на стоимость материализованных рисков в пределах зарезервированной суммы. Наиболее **сложными переговорными точками здесь являются два фактора**: (i) степень автономности (автоматизм) «технической» реализации механики на стороне покупателя; (ii) порядок определения факта материализации риска и его стоимости. Недостаточная проработка этих вопросов создает широкие основания для споров.

Покупатели стремятся обеспечить себе максимальную дискрецию в **определении стоимости риска**, а также **наибольшую степень автоматизма** механики и комфортные сроки. В целях автоматизации уменьшения цены покупатели нередко используют опционы, если это позволяет гибкость структуры владения активом. Также распространена практика зачета встречных требований покупателя о компенсации продавцом имущественных потерь или убытков в связи с нарушенным обязательством или недостоверностью заверений, против требований продавца об уплате полной цены (часть которой была зарезервирована на случай материализации рисков) за качественный актив, без дефектов, которые необходимо было компенсировать таким образом.

> **В отличие от механики earn-out, направленной на обеспечение прироста стоимости бизнеса, у модели holdback иное экономическое целеполагание — обеспечить защиту покупателя от материализации уже имеющихся рисков, стоимость которых не была учтена в цене сделки напрямую, но была перераспределена на продавца с помощью договорных инструментов.**

Реализация механики отложенного платежа требует точного **определения суммы риска**, на величину которого будет произведена корректировка. Продавцы редко соглашаются на использование holdback без предварительного просуживания суммы убытков или потерь, лежащих в основе требования об уменьшении цены. Фактически это означало бы право покупателя изменить цену в одностороннем порядке, несмотря на согласованные в договоре методику и принципы расчета такого уменьшения.

Продавец, не согласный с итоговой величиной расчета, при наличии достаточных аргументов может ее оспорить даже при детальном описании в договоре порядка определения суммы требований покупателя, включая верификацию сторонним оценщиком. Наличие в договоре условия о том, что результат, подтвержденный независимым экспертом, привлеченным сторонами в соответствии с согласованной процедурой, является окончательным и обязательным для сторон, само по себе не препятствует оспариванию размера цены.

В связи с этим механизм отложенного платежа наиболее часто структурируется в сочетании с обязательством продавца компенсировать покупателю подтвержденные судом убытки или потери, которое впоследствии зачитывается против отложенной части цены.

#УМЕНЬШЕНИЕ_ЦЕНЫ



Глеб Тихомиров

советник,
корпоративная практика

LEVEL
Legal services

Среди крупных технологических компаний, выступающих в качестве покупателей, в 2025 г. мы видим растущий тренд на использование инструмента уменьшения цены в сделках по приобретению технологических компаний как гибкого инструмента митигации рисков.

Часто стороны начинают обсуждения с механизма отложенной выплаты в формате earn-out, т. е. выплаты части цены при закрытии сделки и оставшейся части в случае достижения компанией определенных финансовых показателей или результатов (например, запуска продукта). Однако после начала таких обсуждений стороны часто сталкиваются со сложностью структурирования данного инструмента и договариваются о более простых метриках оценки успешности приобретаемого бизнеса через механизм уменьшения цены.

В таких сделках цена является фиксированной, но выплата ее части отложена во времени и фактически «заморожена» как способ закрытия рисков покупателя. Чаще всего такой остаток покупной цены может быть уменьшен на сумму выявленных недостоверностей в финансовой отчетности, требований третьих лиц или выявления обстоятельств возмещения потерь.

В отдельных случаях часть выплаты также откладывается в качестве гарантии того, что ключевые сотрудники останутся в компании и / или будут устранены риски в отношении интеллектуальной собственности в течение переходного периода.

Ключевой особенностью такой «заморозки» является то, что условия выплаты цены или ее уменьшения используются в дополнение к традиционным инструментам защиты покупателя и требуют точного определения для снижения рисков споров в будущем.

#УМЕНЬШЕНИЕ_ЦЕНЫ



Сергей Ханаев

партнер

АЛРУД

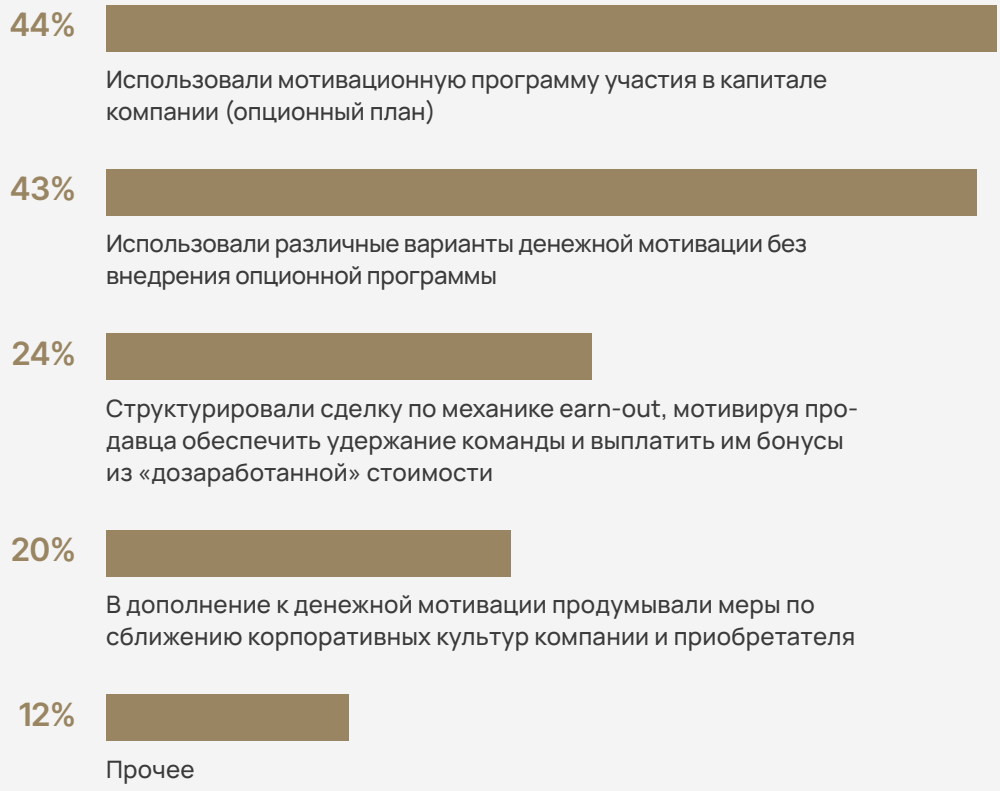
В одной из сделок с технологическим бизнесом в 2025 г. операция уменьшения цены и соответствующая формула были привязаны к возникновению налоговых претензий в связи с потерей статуса резидента Сколково и / или налоговых льгот для ИТ-компаний. Покупатель вместо возмещения налоговых потерь хотел компенсировать их через уменьшение покупной цены, чтобы не создавать дополнительных налогов.

3.2.4 Удержание команды и защита от переманивания

Одной из наиболее важных задач при структурировании сделок в сегменте tech является сохранение ключевой команды после закрытия сделки. Поиску оптимального решения этой проблемы традиционно уделяется большое внимание на переговорах. В ходе онлайн-опросов мы попросили участников отметить, какие подходы к мотивации команды приобретаемой компании они используют в сделках с технологическими активами и какие инструменты защиты от переманивания работников они считают наиболее эффективными.

#РЕЗУЛЬТАТЫ_ОПРОСОВ

Какую систему мотивации команды приобретаемой IT-компании вы наиболее часто использовали в сделках Tech M&A?



По данным Опроса по аспектам Tech M&A (41 респондент).

#УДЕРЖАНИЕ_КОМАНДЫ



Сергей Ханаев

партнер

АЛРУД

Для целей удержания команды после закрытия сделки предусматривались дополнительные мотивационные выплаты ключевым членам команды, размеры и выплата которых зависели от выполнения критериев для earn-out; премии для удержания (retention bonus) для ключевых членов команды, выплачиваемые при условии отработки не менее определенного срока после закрытия сделки. Также иногда продавец остается с миноритарной долей в таргете, чтобы сохранять мотивацию на рост стоимости таргета.

#УДЕРЖАНИЕ_КОМАНДЫ



Артем Тамаев

партнер корпоративной практики и M&A

BETTER CHANCE

Наиболее распространенным является внедрение ESOP программ (например, с использованием фантомных акций или, в случае участия публичной компании в сделке, акций такой публичной компании) для финансовой мотивации сохранения команды. Мы также видели использование механизмов дополнительного финансового поощрения (например, бонусов) в случае реализации определенных событий (например, отсутствия обстоятельств, которые квалифицировали бы работника как ‘bad leaver’) или достижения определенных KPI командой или ее сотрудниками.

#РЕЗУЛЬТАТЫ_ОПРОСОВ

Какие инструменты защиты от переманивания команды вы наиболее часто использовали в сделках Tech M&A?



По данным Опроса по аспектам Tech M&A (41 респондент).

#МНЕНИЕ_ЛИДЕРОВ_РЫНКА

Защита таргета от переманивания сотрудников в сделках Tech M&A: рабочие инструменты



Александр Шалаев
партнер корпоративной практики

ELWI

Защита команды таргета от переманивания, по нашему опыту, зачастую является важным переговорным вопросом в процессе согласования транзакционной документации по M&A сделке в технологической сфере. Инвестор или покупатель, как правило, стремятся максимально широко ограничить все возможные сценарии переманивания, привлечения в качестве подрядчиков и прочие формы взаимодействия продавца с сотрудниками таргета после завершения сделки. Продавец, в свою очередь, стремится максимально ограничить данные механизмы как с точки зрения их «ширины», так и с точки зрения сроков их действия и своей ответственности.

Что касается юридических механизмов защиты от переманивания, в нашей практике в сделках Tech M&A в качестве инструментов защиты таргета от переманивания соответствующих сотрудников (которые были определены путем указания конкретных работников или категорий работников определенного уровня) использовались:

- положения о возмещении потерь, связанных с переманиванием сотрудников таргета при том, что размер соответствующих потерь был привязан к вознаграждению сотрудников за определенный период;
- обязательства продавца (стороны СП) не совершать соответствующие действия по переманиванию или по содействию переманиванию работников, включаемые в корпоративные договоры. Такие положения, как правило, не обеспечивались какими-либо дополнительными обеспечительными механизмами в виде неустойки или опциона.

Исходя из нашего опыта мы видим, что коммерческая команда стороны, приобретающей или сохраняющей контроль над таргетом, практически всегда настаивает на включении в транзакционные документы положений о защите таргета от переманиваний независимо от размера доли, приобретаемой по сделке. Такие положения обосновываются необходимостью сохранения кадров, которые наравне с IT-решениями представляют собой ключевой актив таргета и обеспечивают продолжение бизнеса после закрытия сделки. В случае сделок с положениями earn-out и поэтапным приобретением доли в бизнесе стороны согласовывали действие таких положений, в том числе в течение определенного периода после консолидации покупателем 100%-ной доли в таргете.

#УДЕРЖАНИЕ_КОМАНДЫ



Сергей Колобов

советник

NIKOLSKAYA consulting

Риски переманивания ключевых сотрудников таргета наиболее актуальны в ситуации, когда покупателем является конкурент или потенциальный конкурент, и менее релевантны в ситуации, когда покупатель — это институциональный инвестор.

Если говорить об эффективных механизмах защиты от переманивания, то в рамках российского законодательства мы упираемся в довольно жесткие требования трудового права, которое запрещает ограничение свободы работника на выбор места работы. Любое соглашение подобного рода вряд ли будет исполнимо в российских судах. Тем не менее, существуют юридические механизмы, которые позволяют «работать» с риском переманивания. В частности, в одной из наших сделок мы использовали соглашение по иностранному праву, которым регулировались взаимные обязательства сторон в отношении конкуренции и переманивания сотрудников. Здесь необходимо оговориться, что эффективность такого соглашения зависит от места его принудительного исполнения (в России возможность принудительного исполнения может быть существенно ограничена в силу уже упомянутых особенностей законодательства).

Еще одним «рабочим» инструментом защиты от переманивания является долгосрочная программа мотивации сотрудников, которая будет стимулировать сотрудников продолжать работать в таргете, например, посредством отложенных бонусов или вестинга «фантомных» акций. В этом и прошлом году мы помогали нашему клиенту с подготовкой нескольких таких программ, в том числе чтобы стимулировать сотрудников участвовать в достижении группой долгосрочных бизнес-целей.

#УДЕРЖАНИЕ_КОМАНДЫ



Артем Тамаев

партнер корпоративной практики и M&A

BETTER CHANCE

Одним из самых действенных способов «защиты» команды в ИТ-активе от переманивания является создание финансовых стимулов для текущей команды (например, ESOP программы или иных финансовых бенефитов). Также возможна привязка определенных событий по сделке (например, увеличение или уменьшение доли владения, реализация дефолтного опциона и т. д.) к факту наступления или ненаступления какого-либо события, связанного с командой или ее конкретными людьми.

3.2.5 Специфика заверений и процедуры раскрытия информации

Результаты опроса[3] показали, что в 2025 г. при использовании компенсационных инструментов, в частности, заверений, **стороны Tech M&A-сделок стали чаще учитывать особенности IT-активов**, а также принимать во внимание **рост ИБ-рисков**. Повышенное внимание инвесторов к «технической стороне» бизнеса в 2025 г. было обусловлено не только общим снижением риск-аппетита, но и изменением бизнес-логики. Покупатели, особенно стратегические игроки, в 2025 г. инвестировали не столько в потенциал роста активов, сколько в его реальную способность заполнить конкретные технологические ниши и внутренние функциональные «пробелы», решить специфические IT-задачи. В связи с этим особое значение приобретает соответствие заявленных характеристик продукта реальности. Запрос на усиление IT-специфики в формулировках стандартных механизмов транзакционной защиты в 2025 г. стал ожидаемым последствием развития тренда на повышение интереса к прединвестиционной технической экспертизе IT-продуктов.

В 2025 г. стороны Tech M&A сделок стали чаще использовать более специфические заверения, покрывающие технические аспекты функционирования продукта (отметили **41% респондентов**), а также вопросы ИБ-комплаенса (**29% респондентов**).

В связи с ростом рисков в сфере ИБ и развитием тренда на ужесточение ответственности за утечки в 2025 г. инвесторы стали внимательнее анализировать соответствующие аспекты деятельности приобретаемых бизнесов. На этапе due diligence покупатели запрашивали больше информации по вопросам, связанным с ИБ-инцидентами, утечками, техническими мерами, направленными на защиту внутренних систем от киберугроз, наличием в компании процедур, регламентирующих доступы к различным категориям данных и порядок реагирования на инциденты. Эти вопросы в 2025 г. стали чаще привлекать внимание не только стратегических, но и финансовых инвесторов, которые обычно не интегрируют актив в свой контур и не имеют достаточных инструментов влияния на уровень информационной безопасности продукта.

На стадии подготовки и согласования документов по сделке покупатели чаще просили продавцов предоставить гарантии в отношении параметров информационной безопасности систем, факторов, влияющих на ИБ-риски, характеристик работоспособности и масштабируемости продукта. Если продавец не был готов дать широкие заверения по этим аспектам, покупатели настаивали на уточнении соответствующих обстоятельств в рамках письма о раскрытии и стремились обеспечить максимально возможный уровень контроля над этими вопросами с помощью иных договорных инструментов.

[3] См. результаты опроса на стр. 82 исследования.



Роман Прудентов

партнер

STONEBRIDGE LEGAL

В 2025 г. в рамках предсделочных проверок применительно к ИТ-активам мы видели особый интерес покупателей к следующей информации о приобретаемом таргете и ИТ-активе: (i) информации об инцидентах кибербезопасности (включая сбои и недоступность ИТ-активов, несанкционированный доступ третьих лиц, а также внешние атаки) с запросом покупателя по предоставлению ему детального описания таких инцидентов, причин их возникновения и принятых таргетом мер защиты; (ii) информации о правах, контроле и доступе таргета к аккаунтам и профилям в цифровых сервисах и платформах, используемых для эксплуатации и продвижения ИТ-актива и (iii) информации о включении ИТ-актива в реестр российского программного обеспечения (где это было применимо).

В дальнейшем подобный интерес покупателей выражался в сделочной документации следующим образом:

1. Включение покупателем широкого объема заверений продавцов в отношении инцидентов кибербезопасности, достаточности мер, принятых в таргете для защиты ИТ-актива от инцидентов кибербезопасности, титулу и доступу таргета к аккаунтам и профилям в цифровых сервисах и платформах, а также правомерности включения ИТ-актива в реестр российского ПО.
2. Предусмотрение ограничений на совершение таргетом сделок с учетными записями в цифровых сервисах и платформах до завершения сделки.
3. Включение обязательства о возмещении потерь на случай исключения ИТ-актива из реестра российского ПО и на случай потери доступа таргета к аккаунтам и профилям в цифровых сервисах и платформах по причинам, возникшим до завершения сделки.

Отдельно отметим, что особый подход к информационным правам в post-completion периоде выбирался в сделках с ИТ-активами, которые предусматривали earn-out, базировавшиеся на доработке существующего продукта или достижении согласованных показателей с использованием ИТ-актива (например, ко-

личество пользователей ИТ-активом или выручка от использования ИТ-актива). В таком случае, в совокупности с сохранением на период выполнения KPI операционного контроля над таргетом у продавца, сделочная документация предусматривала предоставление продавцом и таргетом доступа покупателю к ИТ-активу и инфраструктуре для самостоятельного и независимого от продавца подсчета показателей KPI.



Мария Ларионова

юрист корпоративной практики и M&A

BETTER CHANCE

В зависимости от особенностей ПО / датасетов покупателю могут потребоваться заверения о бесперебойной работе в течение определенного времени и обеспеченности мерами информационной безопасности, поскольку критичным фактором может быть устойчивость к сбоям и внешнему воздействию. Степень детализации таких заверений зависит от уровня технической осведомленности команды покупателя.

Также возрастает роль заверений в отношении происхождения и локализации баз данных, ИТ-продуктов и решений, использованных при их создании. По нашим наблюдениям, в последнее время эта тенденция постепенно усиливается, в том числе на фоне законодательного регулирования.

Такие заверения могут использоваться как самостоятельный и основной инструмент защиты или подкрепляться обязательствами о возмещении имущественных потерь в отношении аналогичных обстоятельств.

3.2.6. Опционные конструкции в сделках Tech M&A

Опционы используются в абсолютном большинстве сделок с технологическими активами в качестве ключевого элемента структурирования, 2025 г. в этом смысле не стал исключением. Популярность опционов в сделках Tech M&A обусловлена многими причинами, главной из которых является их **многоцелевой характер, обеспечивающий гибкость в реализации разнонаправленных экономических интересов сторон**.

Опционы позволяют инвестору:

- использовать транзакционные механики, направленные на сглаживание разногласий по оценке, такие как earn-out и ratchet;
- защитить инвестиции и обеспечить доходность;
- получить возможность консолидации актива;
- эффективнее управлять финансовой и операционной дисциплиной в проекте;
- реализовать гибкий, в том числе постадийный, выход из актива;
- мотивировать продавца на удержание команды;
- распределить риски между инвесторами и основателем;
- урегулировать отношения с партнерами, включая спорные ситуации на разных этапах реализации СП,

и разрешить многие другие вопросы.



Анастасия Духина

старший юрист практики корпоративного права

sll
SL LEGAL

Практически все сопровождаемые нами сделки в технологическом секторе предусматривали наличие опционов, как правило, нескольких. Такие опционы можно условно разделить на штрафные и структурные. Первые предоставляются покупателю для защиты от нарушений со стороны продавца, если он остается в компании. В случае наступления каждого предусмотренного таким опционом триггера (утрата прав на существенные IP-активы, дефолт по кредитным обязательствам, уход ключевых сотрудников, утрата резидентства в особой экономической зоне и многие другие в зависимости от существа бизнеса, изначальной структуры собственности и финансового положения компании) приобретатель вправе продать свою долю продавцу-основателю и получить вложенные в компанию деньги с заранее определенной, как правило, повышенной доходностью. Также к штрафным опционам можно отнести опцион на выход основателя, который нечасто, но предоставляется на случай злоупотребления инвестором своими правами в отношении компании.

К структурным опционам мы относим опционы для увеличения доли приобретателя в случае поэтапного выкупа основателя, опционы для реализации drag-along и т. п., каждый из которых привязан к наступлению согласованных сторонами событий (достижения согласованных KPI, решение инвестора о реализации права на drag-along). Как правило, такие опционы реализуются либо по заранее определенной цене либо исходя из оценки компании на определенный момент времени, подготовленной независимым оценщиком.



Валериан Мамагеишвили

советник

KKMP LEGAL

Опционы — это крайне востребованный инструмент в Tech M&A, особенно при структурировании сложных сделок с элементами поэтапного вхождения инвестора в капитал. Цели их использования зависят от стадии развития бизнеса, распределения долей и договоренностей между сторонами, однако можно отметить следующие общие наблюдения.

Во-первых, опцион-пут с минимальной доходностью остается стандартным инструментом защиты инвестора. На фоне ограниченной ликвидности он позволяет инвестору обеспечить возврат средств либо при ухудшении показателей компании, либо по своему усмотрению по истечении определенного периода.

Во-вторых, штрафные опционы (опцион-колл с дисконтом и опцион-пут с премией) часто применяются при нарушении корпоративного договора — в случае смены контроля, нарушения положений о неконкуренции и пр.

В-третьих, опционы служат базой для структур tag-along и drag-along, а также для урегулирования тупиковых ситуаций (deadlock), когда один из участников получает возможность выкупить долю другого на заранее согласованных условиях.

Наконец, опцион-колл широко используется инвесторами как инструмент «докупа» доли после подтверждения устойчивости бизнеса.



Владислав Лазуткин

старший юрист

ORION

Опционы, используемые для приобретения определенной доли или корректировки ранее приобретенной доли, индивидуальны с точки зрения модели ценообразования и зависят от конкретной модели оценки, аппетитов инвестора в отношении потенциальной доходности актива.

Стороны стараются обеспечить привязку условий опциона к конкретным вычислимым показателям, которые может установить внешний эксперт, устраивающий обе стороны, чтобы сохранить уверенность в возможности реализовать опцион.

Структурирование договоренностей в СП и многоэтапных сделках

Опционы являются незаменимым инструментом при структурировании многоэтапных сделок, включая проекты по созданию СП. Они заключаются на стадии входа в проект и регулируют отношения партнеров на этапе развития СП, обеспечивают гибкость при завершении проекта, позволяя консолидировать долю одному из участников СП, выступают средством регулирования тупиковых ситуаций или корпоративного конфликта между участниками проекта.

В частности, в рамках реализации СП опционы позволяют обеспечить (i) поэтапный вход в сделку, предоставляя инвестору право увеличить размер участия в будущем; (ii) защиту на случай недобросовестного поведения партнера, например, блокировки им принятия ключевых решений и создания «искусственной» тупиковой ситуации; (iii) восстановление баланса интересов в случаев смены контроля в активе; (iv) обеспечение возможности выхода из проекта с возвратом ожидаемой доходности, в том числе в случае нарушения партнером своих обязательств по корпоративному договору с целью создания препятствий для выхода инвестора.



Булат Жамбалнимбуев

партнер и руководитель корпоративной практики

NEXTONS



Ксения Михайлова

советник корпоративной практики

NEXTONS

В нашей практике в 2025 г. опционы применялись в ряде сделок M&A в технологическом секторе, связанных с созданием совместных предприятий или входом новых инвесторов. Основные модели опционов и их параметры были следующими:

1. **Опцион-колл (мажоритария) на долю миноритария.**

   Цель: защита мажоритарного участника от блокирования ключевых решений.

   Триггер: отказ миноритария от утверждения кандидатуры генерального директора, предложенной мажоритарием.

   Оценка актива: номинальная стоимость доли.

2. **Опцион-колл (участника) на долю другого участника.**

   Цель: предоставление гибкого права на увеличение доли в проекте.

   Триггер: реализация по инициативе держателя опциона в оговоренный период (без специфических событий).

   Оценка актива: рыночная стоимость, определяемая независимым оценщиком из согласованного сторонами списка.

3. **Опцион-колл (на всю долю) при смене контроля.**

   Цель: защита от нежелательного изменения состава акционеров / участников.

   Триггер: смена контроля.

   Оценка актива: номинальная стоимость доли.

4. **Опцион-пут (на продажу всей доли) при блокировке отчуждения.**

   Цель: гарантия ликвидности для участника, желающего выйти.

Триггер: неполучение необходимого согласия другого участника на продажу доли (если продажа соответствует параметрам, предусмотренным корпоративным договором).

Оценка актива: цена планируемой продажи третьему лицу.

5. **Опцион-пут (на продажу всей доли) при нарушении права совладения (tag-along).**

   Цель: защита прав участника, лишенного возможности продать свою долю совместно с другим участником.

   Триггер: нарушение процедуры tag-along другим участником при продаже им своей доли.

   Оценка актива: цена, рассчитываемая по формуле для продажи доли покупателю в нарушенной сделке.

Консолидация владения активом

Одной из ключевых целей использования опционов в сделках с технологическими активами в 2025 г. было структурирование многоэтапных сделок. Наиболее распространенным пакетом участия в активе, приобретаемым стратегическим инвестором в рамках первичного входа в сделку, была доля в размере ниже контрольной. Опционы-колл обеспечивали инвестору возможность увеличить долю участия стратегического инвестора в активе в будущем. Конечной точкой консолидации в большинстве случаев является 100% доля участия в бизнесе, что позволяет остальным инвесторам и основателям реализовать выход из актива.

Во многих случаях право инвестора на приобретение дополнительной доли не обусловлено наступлением какого-либо события или обстоятельства и «привязано» лишь к определенному сроку. Это дает возможность инвестору беспрепятственно реализовать право на консолидацию актива, если им будет принято такое решение. Чаще всего такие опционы реализовывались по рыночной стоимости актива. В случае ухудшения ситуации в бизнесе или неподтверждения проверяемых гипотез инвестор мог сохранить статус-кво в активе, реализовать опцион-пут на продажу всей имеющейся доли (при наличии в структуре такого опциона) или сбалансировать цену через механизм рэтчета, сохранив участие в бизнесе.



Сергей Капустин

партнер практики корпоративного права

Melling Voitishkin &Partners

Опционы активно использовались в Tech M&A сделках в 2025 г.

В одной из сделок ключевой целью опциона являлась консолидация владения активом. Опцион предоставлял инвестору возможность в будущем увеличить свою долю в таргете до 100%, выкупив оставшиеся доли у основателей бизнеса.

Триггером для исполнения опциона служил временной фактор: опцион мог быть реализован инвестором только по истечении нескольких лет с момента закрытия первоначальной сделки.

Стоимость доли по опциону определялась как наименьшее из двух значений:

1. рыночная оценка приобретаемой доли на дату реализации опциона, проведенная независимым оценщиком; либо
2. цена, рассчитанная по формуле на основе финансовых показателей таргета на дату реализации опциона (показатели Revenue и EBITDAC, умноженные на соответствующий заранее согласованный мультипликатор).



Софья Смирнова

советник M&A и корпоративной практики

O_2 консалтинг

По нашему опыту опционы использовались для приобретения инвестором контрольной доли в активе по истечении определенного периода времени при успешном развитии событий (как механизм получения фаундерами вознаграждения) — право на реализацию опциона-колл предоставлялось по истечении определенного срока существования совместного предприятия, и цена доли была привязана к финансовым показателям бизнеса на момент реализации опциона (выручка с коэффициентом).

Удержание команды

Успешность развития многих технологических активов существенно зависит от роли их основателей и команды. Поэтому многие сделки в сегменте tech структурируются таким образом, чтобы сохранить участие основателя в капитале компании на максимально возможный срок вплоть до итоговой точки реализации проекта, например, IPO или продажи стратегическому инвестору. Даже если стратегический инвестор уже на первом этапе сделки приобретает контролирующую долю, но при этом используется механика earn-out, — основатель в большинстве случаев сохраняет миноритарное участие в активе, как минимум, на период earn-out. Такой подход позволяет не только мотивировать команду на продолжение активного развития проекта после входа инвестора, но и предотвратить создание конкурирующих бизнесов и утечек ценной коммерческой информации.

У стратегических инвесторов практически отсутствуют какие-либо инструменты эффективного влияния на действия команды до завершения процесса интеграции бизнеса в свой контур. В силу законодательных ограничений не существует и каких-либо эффективных механизмов, позволяющих гарантированно удержать ключевых работников в компании в течение определенного периода. В связи с этим опционы часто используются в качестве инструмента мотивации основателя и — одновременно — страховочного механизма, выступая средством косвенного влияния на поведение команды компании.



Константин Саврыга

юрист

NIKOLSKAYA consulting

Опционы являются одной из самых незаменимых конструкций в сделках Tech M&A, так как такие сделки редко предполагают единоразовое приобретение 100% контроля и полный выход текущих владельцев. Это обусловлено тем, что одним из самых главных активов таргета, как правило, является даже не само ПО, а команда, ключевые члены которой являются владельцами таргета.

В такой ситуации в интересах покупателя удержать старую команду и обеспечить их commitment на определенный период. В случае продажи 100% долей в таргете существует риск того, что команда будет более заинтересована в своих новых проектах, в которые будут инвестированы полученные средства, чем в таргете.

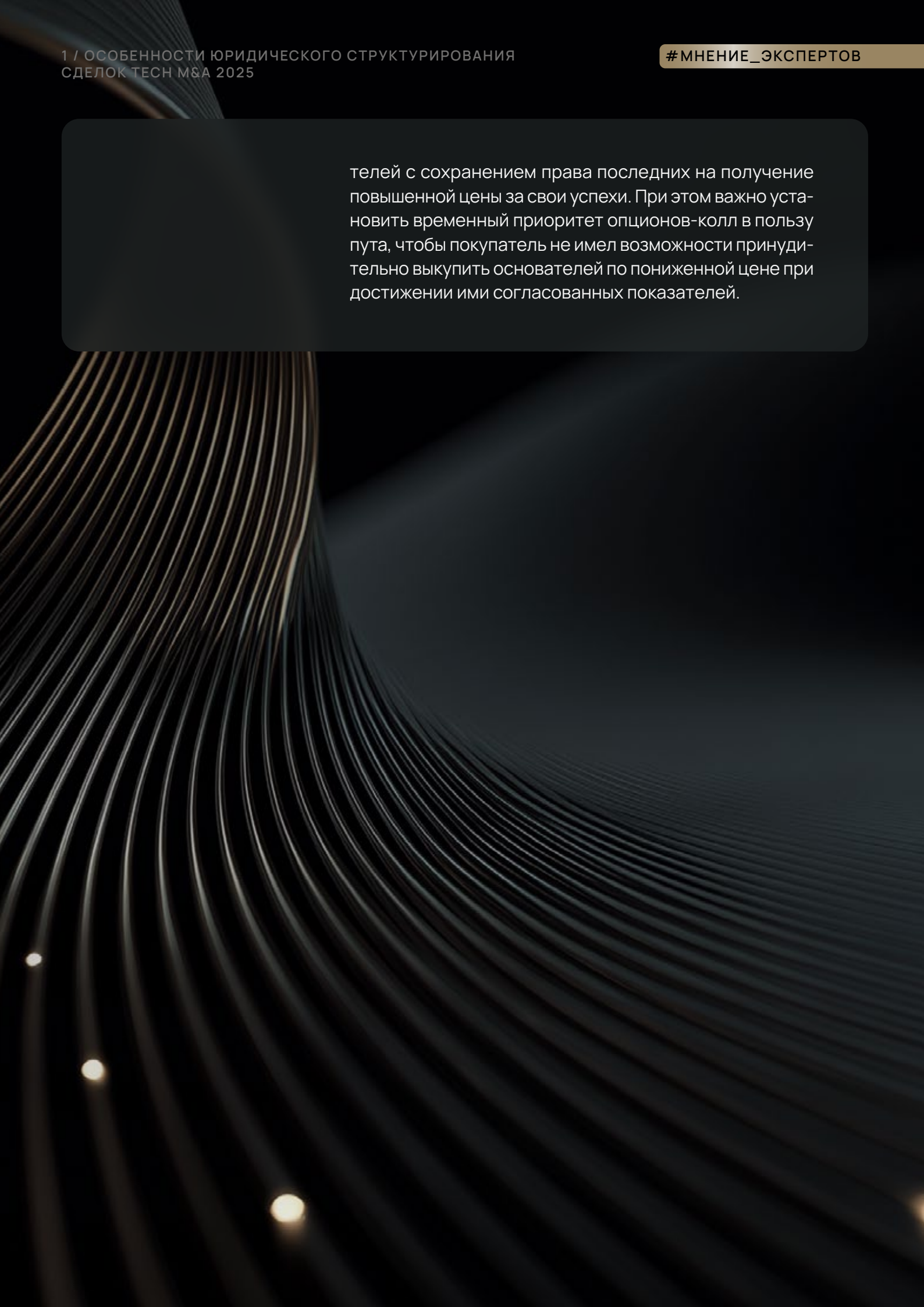
Для минимизации указанного риска покупателю целесообразно структурировать сделку в несколько этапов:

- приобретение контрольной доли на основании согласованной сторонами консервативной оценки,
- выплата earn-out за ранее приобретенную долю в течение короткого периода (1-2 года) и
- последующий стадиальный выход через опционы-колл и пут.

Так как выход основателей является заранее определенным и весь вопрос состоит лишь в цене выкупаемых долей, то стадиальный выход лучше структурировать через зеркальные опционы (колл покупателя и пут продавца). Опционы-колл покупателя являются безусловными и позволяют ему выкупить всю или часть оставшихся долей основателей по минимальной согласованной оценке в определенные даты. Опционы-пут продавцов, напротив, направлены на предоставление продавцам права продать всю или часть своей доли при выполнении согласованных показателей, при этом оценка по опционам-пут устанавливается выше, чем по коллам.

Такая комбинация позволяет обеспечить гарантированный контролируемый покупателем выход основа-

телей с сохранением права последних на получение повышенной цены за свои успехи. При этом важно установить временный приоритет опционов-колл в пользу пута, чтобы покупатель не имел возможности принудительно выкупить основателей по пониженной цене при достижении ими согласованных показателей.



Защита инвестиций и обеспечение доходности

Опцион является одним из ключевых инструментов, используемых финансовыми инвесторами в целях обеспечения возврата инвестиций с доходностью. Многие технологические бизнесы нуждаются в инвестициях на поддержание текущей ликвидности и масштабирование. Единственной альтернативой акционерного финансирования, как equity, так и заемного, для них является сделка cash-in с внешним инвестором. Если инвестиции предоставляет финансовый инвестор, они являются относительно краткосрочными и имеют определенную таргетированную доходность, которую инвестор хотел бы получить по окончании своего участия в проекте. Для этих целей инвесторы активно используют опционы-пут, обеспечивающие возможность продажи своей доли основателям бизнеса с премией, то есть по цене с учетом оговоренной доходности на вложенные инвестиции.

Владельцы активов не всегда охотно соглашаются на включение в структуру сделки опционов-пут финансовых инвесторов, это часто является важной точкой переговоров. Такой опцион — очень сильный инструмент, реализация которого в будущем в ряде случаев может ухудшить финансовое положение основателя и компании. Однако высокая стоимость финансирования и отсутствие доступа к его альтернативным источникам все чаще вынуждают основателей соглашаться на использование таких опционов, эта тенденция была отмечена многими участниками Tech M&A сделок в 2025 г.

Также, по оценкам экспертов, в 2025 г. усилился тренд на использование т. н. дефолтных или штрафных опционов как средства регулирования отношений между партнерами и управления поведением миноритарных участников. Основная цель таких опционов — недопущение недобросовестных действий со стороны других участников, которые могли бы воспрепятствовать реализации намерений стратегического инвестора, выкупившего контрольную долю в активе, или компании в целом. В таких случаях могут использоваться как опционы-пут с премией к цене реализации, так и колл — с дисконтом. Нередко цена в опционах-колл носит символический характер и устанавливается в размере номинальной стоимости. Эта практика получила широкое распространение в 2025 г., поскольку наличие таких опционов в структуре сделки обеспечивает эффективный мотивирующий эффект в отношении участников, от которых может зависеть успех реализации проекта и рост его стоимости. Эта тенденция отражает влияние динамики «рынка покупателя» на выбор транзакционных средств защиты инвестиций в условиях макроэкономической нестабильности. Однако при использовании таких опционов следует тщательно оценивать риски их возможной переквалификации в неустойку с возможностью ее снижения, а также налоговые последствия реализации соответствующих операций.



Валериан Мамагеишвили

советник

KKMP LEGAL

Выбор инструментов выхода и обеспечения доходности для equity-инвестора в IT-секторе во многом зависит от стадии развития таргета и структуры cap-table. На ранних этапах (pre-seed, seed) приоритет, в частности, отдается механизмам конвертации, в то время как на более поздних стадиях чаще применяются комбинированные конструкции, включающие опцион-пут как инструмент возврата инвестиций с минимальной доходностью.

Практика показывает, что опционы-пут с заранее согласованным IRR-порогом нередко воспринимаются инвесторами как вполне оправданная форма защиты инвестора, особенно в условиях ограниченной ликвидности рынка. Для существующих акционеров и основателей такой инструмент зачастую является вынужденной уступкой, обеспечивающей доступ к финансированию на приемлемых условиях. При этом общее отношение текущих участников к опционам пут остается настороженным, т. к. в случае неудачного сценария выполнение обязательств по опциону может оказаться неподъемным обязательством.

С юридической точки зрения важно помнить, что опцион-пут создает лишь право требования, но не гарантирует фактическое получение согласованной суммы. Если контрагентом по нему выступает физическое лицо-основатель, чьи активы ограничены долей в компании-таргете, реализация опциона при снижении стоимости бизнеса может привести к его неплатежеспособности. Поэтому при использовании пут-опциона ключевым становится анализ платежеспособности опционодателя и проработка соответствующего обеспечения.



Анастасия Духина

старший юрист практики корпоративного права

sll
SL LEGAL

В нашей практике наиболее эффективным инструментом выхода финансового инвестора является пут-опцион, который позволяет вернуть долю основателю без его существенного вовлечения и в то же время фиксирует цену такого возврата с учетом желаемой доходности. Основатели в большинстве случаев в целом не возражают против такого механизма, однако довольно сложно согласовывают триггеры и сроки для реализации опциона. При наличии инвесторов предыдущих раундов согласование условий опциона обычно требует учета интересов этих инвесторов, поскольку зачастую они тоже имеют опционы со схожими триггерами, а реализация одновременно всех опционов может привести к неплатежеспособности основателя.

Корпоративное управление и правила консолидации

Многие сделки M&A с технологическими активами структурируются в несколько этапов. В ряде случаев стратегическому покупателю удается согласовать приобретение контролирующей доли уже на первой стадии сделки и получить явно выраженные контрольные полномочия, предоставляемые фактом владения долей соответствующего размера. В таких случаях у миноритарных участников могут сохраняться «уравновешивающие» полномочия «негативного» контроля.

В 2025 г. ситуация в сделках сегмента tech несколько изменилась в сторону снижения размера долей, приобретаемых стратегическими покупателями на первом этапе сделки. Как отмечают аналитики рынка, в 2025 г. наиболее распространенным пакетом первичного приобретения являлась доля в диапазоне «существенного влияния», но не контроля. Эти заключения основаны преимущественно на оценке размера прямого или косвенного корпоративного участия в капитале приобретаемой компании и не учитывают набор договорных механизмов, обеспечивающих приобретателю доли дополнительные полномочия по контролю. Такая информация является закрытой и по этой причине не принимается во внимание в рамках соответствующего анализа.

Ситуации, в которых «плавающий» размер пакета и многоэтапность сделки дополняются существенным набором полномочий приобретателя в рамках транзакционной документации являются сложными для корректного применения правил учета приобретения актива и составления консолидированной отчетности. МСФО 3 и 10, посвященные вопросам учета приобретений по итогам сделок M&A и подготовки консолидированной финансовой отчетности (соответственно), оперируют сложной терминологией, включающей понятие контроля и существенного влияния, правильное толкование которых имеет важное значение для корректного учета соответствующих операций.

Если приобретатель стремится консолидировать актив уже на первом этапе сделки, необходимо внимательно анализировать набор полномочий партнеров по сделке, «балансирующих» возможности приобретателя. Если другие участники бизнеса сохраняют существенные полномочия, это может быть истолковано как препятствие для признания контроля и консолидации актива на текущем этапе сделки.



Константин Саврыга

юрист

NIKOLSKAYA consulting

Помимо своего основного назначения опционы могут применяться в качестве инструмента структурирования корпоративного управления в таргете.

При приобретении таргета для многих стратегических игроков приоритетной является не только интеграция его продукта в свою экосистему, но и обеспечение консолидации таргета в финансовой отчетности группы покупателя.

Это делает невозможным отражение в уставе или корпоративном договоре ряда классических требований основателей, таких как сохранение операционного контроля, необходимого для обеспечения справедливой цены по earn-out и стадиальному выходу по опционам, или обязательств по распределению прибыли в пользу основателей не ниже определенного размера.

В таких ситуациях договоренности сторон могут быть закреплены не в виде обязательства сделать что-то, а в виде права основателей выйти из проекта путем реализации своего опциона-пут при наступлении согласованных триггеров, например, назначения генерального директора не из основателей или распределение прибыли ниже согласованного порога.

Такой подход позволит создать сдерживающий фактор на стороне покупателя, который заставит его соблюдать достигнутые договоренности, но при этом удовлетворить все требования к консолидации таргета.

Чрезвычайно важным является определение ценовой механики опциона-пут, так как она, с одной стороны, должна служить сдерживающим фактором для покупателя, препятствующим нарушению договоренностей, а с другой не закрывать возможность принудительного отстранения основателей от управления в случае, если это коммерчески оправданно.

Другим важным моментом ценовой механики является синхронизация оценок до входа покупателя и на этапах последующей реализации опционов. Так, таргеты часто

используют отчетность по РСБУ, а их оценка делается на основании существенного количества корректировок, а после входа покупателя таргет часто переходит на МСФО. Основатели же в результате необходимости соблюдения требований консолидации или уже осуществленного частичного выхода могут утратить контроль над принятием учетной политики, что создает риск искажений в оценке. Для нивелирования указанного риска стороны могут согласовать основные принципы оценки в документах по сделке или даже приложить согласованную сторонами учетную политику.

3.2.7. Инструменты защиты финансовых инвестиций

Как показали результаты опроса[4], среди общего объема сделок, по которым в 2025 г. приобретались **миноритарные доли**, преобладали пакеты **существенного влияния** (от 35% до 49% участия в капитале). Значительную долю также составляли пакеты участия **от «супер»-миноритарного до блокирующего** (от 10% до 35% участия в капитале актива. Для инвестиций, совершаемых финансовыми инвесторами, характерны оба указанных формата, они редко приобретают контрольные пакеты, в том числе целях соблюдения требований учета. Для классических финансовых инвестиций наиболее характерен формат блокирующего пакета, предоставляющего полномочия «негативного» контроля.

Стандартные средства защиты (protective provisions) интересов финансового инвестора, владеющего неконтрольной долей в активе, помимо тех, что характерны для любых типов инвестиций, условно можно разделить на три категории. Это инструменты, обеспечивающие:

- контроль за инвестициями (специфические reserved matters и защита от вывода ключевых активов, информационные права, назначение финансового контролера или CFO, место в совете директоров);
- корректировку стоимости и размера доли, в том числе при понижающем раунде (антиразмывочные положения / рэтчеты, опционы);
- опции выхода и обеспечения доходности (опцион-пут, ликвидационная привилегия, обеспечение платежа).

Объем полномочий финансовых инвесторов по управлению активом обычно сосредоточен вокруг вопросов финансирования и стратегического развития компании. Однако в 2025 г. им все чаще приходилось погружаться на операционный уровень, в частности, в вопросы контрактации и продаж, расширения клиентского контура.

В 2025 г. широкое распространение получили сделки с участием синдикатов equity-инвесторов. Это более сложная конфигурация cash-in инвестиций, при которой разные инвесторы в составе консорциума могут консолидировать позицию и реализовывать определенные средства защиты в коллективном формате. Такие структуры требуют особо тщательной синхронизации интересов всех участников.

[4] См. общие результаты опроса на стр. 42–23 исследования.



Арташес Оганов

партнер, глава практики корпоративного права / M&A

sll

Как правило, объем прав и защитных механизмов зависит от статуса и целей приобретателя. В сделках, где приобретатель (даже существенного пакета) является финансовым инвестором, контроль за операционной деятельностью и, соответственно, ИТ-активами остается у основателей. В этом случае главная защита — это предварительные и последующие условия в отношении «исправления недочетов», выявленных в процессе due diligence, заверения об обстоятельствах и возмещение имущественных потерь, а также возможность реализовать штрафной пут-опцион в случае существенных проблем с основными ИТ-активами. В сделках, где компания приобретается для последующей интеграции в бизнес покупателя, к перечисленным выше инструментам, как правило, добавляется значительный объем reserved matters в отношении распоряжения ключевыми активами, отношений с основными контрагентами и т. п., а также возможность корректировки покупной цены по earn-out в случае выявления проблем или недостижения согласованных KPI.

При приобретении блокирующего или супер-миноритарного пакета тенденции такие же, как и описанные, только объем предоставляемых заверений, контроля и возможности корректировки цены, как правило, меньше, поскольку миноритарный акционер / участник априори имеет меньше контроля и вовлечения в деятельность компании. Исключением, однако, являются сделки либо с поэтапным выкупом основателя, в которых объем защиты приобретателя либо сразу устанавливается на довольно высоком уровне (как описано выше), либо постепенно растет по мере увеличения доли в компании (например, возможность блокировать определенные решения или контролировать назначение определенных сотрудников появляется после превышения согласованного порога владения.

Поиск подходящей опции выхода из проекта в 2025 г. стал для финансовых инвесторов также более сложной задачей. Продажа доли через tag-along, как и ранее, могла сработать лишь в единичных случаях и не являлась базовым сценарием. Финансовым инвесторам приходилось активнее искать крупного игрока, которому был бы интересен актив в целом. В 2025 г. стратегические инвесторы реже приобретали контрольные пакеты, и тем более весь актив, в рамках первого этапа сделки. Для оценки эффективности и тестирования гипотез было достаточно неконтрольной доли. Финансовым инвесторам приходилось адаптировать инвестиционные цели и принимаемые решения к продолжительному «сожительству» с крупным партнером, на которого возлагались ожидания по консолидации актива в будущем и обеспечению возможности выхода.

Это в ряде случаев приводило к пересмотру объема и характера стандартных инструментов защиты финансовых инвестиций (рэтчеты, ликвидационные привилегии, права вето, опционы-пут, непропорциональное распределение прибыли и т. п.) и их более гибкой оптимизации с учетом интересов стратегического партнера.

3.3 Актуальные подходы к управлению рисками в сделках Tech M&A 2025

В рамках онлайн-опросов мы попросили участников сделок Tech M&A отметить, изменились ли в 2025 г. подходы к управлению рисками и фокус внимания инвесторов к их анализу.

#РЕЗУЛЬТАТЫ_ОПРОСОВ



Считают, что в 2025 г. инвесторы при приобретении технологических компаний стали более требовательными к анализу и управлению рисками в целом.



Считают, что покупатели стали тщательнее анализировать юридические риски, связанные с ключевым ПО и данными.

По данным Опроса по структурированию сделок Tech M&A в 2025 г.

Как показали итоги опросов, многие участники рынка отметили, что **в 2025 г. покупатели стали строже оценивать риски IT-бизнесов**, включая юридические и регуляторные. Это связано с общим трендом повышения требований к качеству и риск-профилю приобретаемых активов в 2025 г. на фоне сложной макроэкономической ситуации и появления новых вызовов и угроз в сфере IT.

#РЕЗУЛЬТАТЫ_ОПРОСОВ

Изменился ли подход к управлению юридическими рисками в сделках Tech M&A в 2025 г.?



По данным Опроса по структурированию сделок Tech M&A в 2025 г. (125 респондентов).

Существенная доля респондентов (**43–58%**) отметили, что **значимым трендом 2025 г. стало усиление внимания инвесторов к проверке юридических рисков** приобретаемых IT-компаний. При этом около четверти опрошенных (**22% респондентов**) в 2025 г. не увидели каких-либо существенных изменений в подходах к управлению рисками при приобретении IT-активов, а **6% респондентов** столкнулись с их упрощением.

Как отметили многие эксперты, а также опрошенные нами участники исследования, **в 2025 г. фокус юридического анализа IT-компаний стал более широким**. Это связано не только с возросшими требованиями инвесторов к качеству активов, но и с ужесточением регулирования в ИТ-сфере, отменой мораториев на проверки, развитием технологий и необходимостью решения новых бизнес-задач.

Особое значение в 2025 г. приобрела проверка титульных рисков. Несмотря на их традиционную актуальность, на фоне снижения оценок IT-бизнесов эти вопросы, особенно в продуктовом сегменте, вновь вышли на первый план. Распространение технологии вайб-кодинга (генерации программного кода с помощью ИИ-инструментов) также привело к необходимости проверки фрагментов кода, сгенерированных нейросетями.



Вячеслав Поджаров

старший менеджер проектов инвестиционного банка

ADVANCE CAPITAL

Одними из наиболее значимых рисков для инвесторов стали вопросы утечек данных и информационной безопасности, а также вопросы, связанные с использованием зарубежного ПО. Именно эти факторы напрямую влияют на возможность дальнейшего использования продукта, его интеграцию в контур покупателя и устойчивость финансовых показателей без больших рисков.

Особенно заметно смещение фокуса от формальной проверки документов к оценке реальной защищенности актива. Покупателю важно понимать не только то, кому юридически принадлежат права на продукт, но и как этот продукт создавался, какие подрядчики и сотрудники участвовали в разработке, какие open source компоненты использовались, есть ли ограничения по данным, не нарушаются ли требования в области персональных данных и информационной безопасности.

Наличие сильного продукта и растущей выручки не компенсирует неоформленные права на код или неочищенный регуляторный периметр. Юридические риски в Tech M&A все чаще становятся не только предметом гарантий и заверений, но и фактором, который влияет на цену, структуру оплаты, перечень отлагательных условий и готовность покупателя закрывать сделку.

Как показали результаты онлайн-опросов[5], посвященных проблематике управления рисками в сделках Tech M&A, **негативные последствия, связанные с оспариванием титула на ключевое ПО** приобретаемой компании, являются:

- **типовыми и наиболее распространенными (88% респондентов);**
- **критичными, способными повлиять на судьбу сделки (93% респондентов);**
- **поводом для переговоров об отказе от сделки (80% респондентов);**
- **приоритетным направлением due diligence IT-компаний (95% респондентов).**

[5] С полными итогами опросов можно ознакомиться в соответствующих разделах главы 2 исследования на стр. 193, 212, 262 и 173 (соответственно).



Алексей Мустяца

директор, управление слияний и поглощений

СОВКОМБАНК

Результаты опроса в части рисков оспаривания титула на ключевое ПО и датасеты Tech-таргетов полностью коррелируют с нашей практикой. В 2025 г. вопросы титула на ПО и базы данных действительно являлись одними из наиболее частых, критичных и потенциально разрушающих сделку факторов и в ряде случаев — определяли структуру сделки и ее исполнимость.

Активный тренд на использование российского ПО и IT-льгот потребовал от инвесторов анализа вопросов, связанных с включением ПО в государственные реестры. Ужесточение ответственности за обработку персональных данных привело к необходимости более тщательной проверки этих процессов. Текущая геополитическая обстановка стала фактором углубленной проверки наличия зарубежных компаний в группе продавца, которые могли бы сохранить контроль над ключевыми активами. Больше внимания стало уделяться санкционным и регуляторным вопросам, использованию ПО ушедших иностранных вендоров и рискам в цепочках поставок.



Антон Джуплин

партнер

АЛРУД

На первый план вышли следующие аспекты юридического DD:

1. Соблюдение контрсанкционного регулирования, в том числе в отношении сделок с интеллектуальной собственностью;
2. Анализ незаконного использования таргетом интеллектуальной собственности третьих лиц (в том числе стороннего ПО), особенно с учетом массового выхода иностранных ИТ компаний с российского рынка;
3. Зависимость таргета от IT-инфраструктуры группы, в которую он входил до сделки;
4. Вероятность утраты возможности использования интеллектуальной собственности третьих лиц ввиду международных санкций (например, резкое отключение от иностранного ПО);
5. Риски применения к таргету законодательства о критической информационной инфраструктуре;
6. Вопросы соблюдения законодательства о персональных данных.

Данные аспекты возникали ранее, однако в 2025 г. наиболее остро встали перед покупателями активов.



Владислав Лазуткин

старший юрист

ORION

В нашей практике сопровождения сделок Tech M&A в 2025 г. в приоритетном порядке приобретатели технологических активов анализировали следующие юридические и регуляторные риски: титул на доли / акции и ключевые активы (в том числе IP), приватизационные риски, регуляторные риски, которые могут оказать влияние на льготы, перспективы бизнеса или финансовую модель (реестр российского ПО, рекламу, статус владельца агрегатора, организатора распространения информации и т. п.), команду и ключевой персонал, обработку персональных и иных типов данных.

Помимо классического пула рисков хотелось бы выделить ряд тенденций:

- повышенное внимание к регуляторным рискам, которое обусловлено следующими трендами: ужесточение регулирования IT-бизнеса в РФ и за рубежом, усиление локализации чувствительных данных и технологий, повышение прозрачности операций и коммуникаций в интернете, формирование суверенного информационного пространства, а также урегулированиея статуса игроков определенного сектора;
- возрастает роль координации команд, осуществляющих legal и tax due diligence (например, некоторые налоговые риски могут вытекать из регуляторных);
- с учетом трансграничной фрагментации бизнеса таргета особую роль в legal due diligence занимает единство в работе команд консультанта, которые работают в РФ и странах присутствия таргета, — это обеспечивает комплексную проверку единого, по существу, бизнеса.

Рост в 2025 г. числа утечек и киберугроз, а также активное распространение ИИ-технологий потребовали от инвесторов более глубокого анализа использования зарубежных информационных систем и связанных с этим уязвимостей.



Елена Полевая

старший юрист

KKMP LEGAL

В 2025 г. в юридической проверке ИТ-бизнесов на первый план вышли риски в сфере защиты данных и применения бизнесом новых технологий (например, искусственного интеллекта).

Для защиты данных прежде всего актуальны киберриски и риски утечки персональных данных.

Количество кибератак в 2025 г. возросло кратно. Только за первые полгода 2025 г. было зафиксировано 63 000 инцидентов, что на 27% больше, чем в 2024 г. Из них 66% кибератак связаны с вредоносным ПО. Это влечет имущественные потери и другие существенные риски для бизнеса, такие как ущерб деловой репутации, остановка бизнес-процессов, утечка критических данных.

Киберриски, актуальные для всех, еще более актуальны для ИТ-бизнеса, использующего критически важную инфраструктуру. Юридическая проверка этих рисков всегда идет рука об руку с IT-аудитом.

В области персональных данных проверка риска утечек данных стала особенно актуальной в свете ужесточения ответственности за нарушения. В объем проверки также стал входить анализ наличия у приобретаемой компании мер контроля по раскрытию работниками персональных данных и конфиденциальной информации при использовании внешних ИИ-моделей.

В области интеллектуальной собственности в юридической проверке появились новые вопросы и новые типы рисков, вызванные использованием технологий ИИ, в том числе нарушение прав интеллектуальной собственности при обучении модели или ее результатах, отсутствие титула на результаты генераций искусственного интеллекта и др. Новые риски для ИТ-компаний принесла и разработка программных продуктов с помощью ИИ-инструментов. В частности, актуальным стал риск утечек данных из-за внедрения вредоносного кода при его разработке ИИ. Также риск применения условий открытых лицензий к программным продуктам приобретаемой компании, созданным ИИ-инструментами. Если модель ИИ была обучена на коде с открытым

исходным кодом, то сгенерированный ИИ исходный код может воспроизводить открытый код, на котором он обучался. К такому коду будут применяться требования открытых лицензий по раскрытию исходного кода, что делает невозможным коммерциализацию созданных ИИ программных продуктов.



Кристина Мкртчян

советник практики интеллектуальной собственности

ЭБР
Юридическая Компания

Подтверждается вывод, что управление юридическими рисками технически ориентированно: на первом месте риски титула на программные продукты и датасеты (58% респондентов), далее идут риски утечек данных и кибербезопасности ИТ-контура (54% респондентов), а также регуляторные и комплаенс-риски (46% респондентов).

Покупателю мало проверить документы: нужно понять, кому принадлежит код, на каких основаниях используются датасеты, как устроена обработка данных, есть ли vendor lock-in и может ли продукт работать после смены контроля.

Подходы к управлению рисками



Считают, что в 2025 г. инвесторы стали чаще требовать устранения рисков до подписания сделки, а не в период между подписанием и закрытием.

По данным Опроса по структурированию сделок Tech M&A.

#РЕЗУЛЬТАТЫ_ОПРОСОВ

По мнению большинства Tech M&A экспертов, в 2025 г. не произошло структурных сдвигов в подходах к управлению рисками в сделках с технологическими активами. При этом существенная доля (**35%**) респондентов онлайн-опроса отметила, что в 2025 г. появился **тренд на максимальное устранение выявленных рисков до подписания документации по сделке**, особенно в отношении прав на ключевое ПО[6].

Значимым трендом 2025 г. стало усиление внимания инвесторов к проверке юридических рисков приобретаемых IT-компаний.

Многие участники сделок Tech M&A также подчеркнули, что в 2025 г. сохранил актуальность традиционный двухуровневый подход к работе с рисками, выявленными в ходе due diligence. На первом этапе стороны обеспечивают реализацию конкретных мероприятий, направленных на фактическое устранение выявленных рисков или смягчение их последствий. В 2025 г. этот процесс нередко становился частью более широкого комплекса действий предпродажной подготовки актива. Те риски, которые по итогам проведения соответствующих мероприятий оставались неурегулированными, стороны старались распределить с помощью договорных инструментов.

[6] Более подробно вопросы митигации рисков ИТ-компаний рассмотрены в главе 2 разделе 2 «Подходы к митигации юридических IT-рисков».

#ПОДХОДЫ_К_МИТИГАЦИИ_РИСКОВ



Булат Жамбалнимбуев

партнер и руководитель корпоративной практики

NEXTONS



Ксения Михайлова

советник корпоративной практики

NEXTONS

Для митигации рисков приобретатели применяют двухуровневый подход, сочетающий фактические меры, предпринимаемые до реализации сделки, и договорные механизмы защиты.

По итогам проведенных проверок и предоставления имеющихся у компании документов в первую очередь компания устраняет выявленные дефекты в оформлении документации. В частности, компания заключает договоры и дополнительные соглашения и подписывает акты приема-передачи с авторами-разработчиками (правообладателями), устраняющие ряд идентифицированных рисков, а также при необходимости вносит изменения в имеющиеся свидетельства о регистрации в части указания реального перечня авторов.

Далее покупатель включает в документацию следующие ключевые механизмы защиты:

- в части, в которой конкретные риски не выявлены, — объемный перечень заверений продавца о титуле, должной передаче прав, действительности договоров-оснований, отсутствии прав третьих лиц, корректности документации (информации) о ПО и датасетах и т. д.;
- в части, в которой выявлены конкретные риски, — обязательства продавца возместить имущественные потери покупателя вследствие отсутствия у компании (прекращения) титула и предъявления к компании претензий и требований со стороны авторов-разработчиков (правообладателей).

Дополнительно покупатель может договориться об уменьшении покупной цены вследствие выявленных рисков, которые при этом не являются критичными и не влекут отказ покупателя от сделки. Данный механизм служит компромиссным инструментом, позволяя частично перераспределить бремя будущих убытков, возложив их на продавца.

По нашему опыту, в 2025 г. непосредственно подход к структурированию механизмов защиты не претерпел

фундаментальных изменений. Однако акцент сместился в сторону усиления проверки до реализации сделки. Покупатели теперь тщательнее отслеживают фактическое устранение компанией описанных выше дефектов в оформлении документации (например, реальное подписание всех актов с разработчиками).

#ПОДХОДЫ_К_МИТИГАЦИИ_РИСКОВ



Владислав Лазуткин

старший юрист

ORION

> Общий подход к митигации рисков в сделках Tech M&A в 2025 г. не изменился.

Разумеется, наши клиенты используют широкий пул и юридических, и технических инструментов. В юридической плоскости используется и pre-closing работа по оформлению разработки, передачи IP, отношений с разработчиками, устранению дефектов титула и т. п., и стандартные инструменты, включаемые в транзакционную документацию (заверения, возмещение потерь, снижение покупной цены). В технической плоскости, например, может быть проведена как глобальная работа по интеграции, так и точечная проработка рисков, например, может быть переписан проблемный код, заменен модуль с некомфортной лицензией и т. п.

В целом отметим, что покупатели могут оставаться толерантны к ряду рисков использования ценных для бизнеса IT-продуктов с нарушением или в отсутствие лицензий с учетом контекста, сложившегося после февраля 2022 г.

Раздел 4

Спецпроект: earn-out — решение проблемы или иллюзия договоренности

АВТОР



Юлия Загорнова
Группа компаний Б1

На рынке M&A earn-out принято считать одним из наиболее действенных инструментов для достижения компромисса в ситуации, когда настрой на сделку есть, но мнения о справедливой стоимости актива расходятся. Когда продавец уверен в потенциале бизнеса и настаивает на более высокой оценке, а покупатель не готов платить сегодня за результаты, которые еще только должны быть достигнуты, стороны находят, как им кажется, рациональный выход: часть цены выплачивается при закрытии сделки, а часть — позже, если компания покажет заранее согласованный результат.

С точки зрения общей логики такая конструкция выглядит вполне понятно. Она позволяет не «развалить» сделку из-за расхождения взглядов на оценку, «сохранить лицо» обеим сторонам и формально объединить две разные точки зрения на оценку одного и того же актива. Но именно здесь и кроется главное заблуждение. Earn-out — это не техническая надстройка в структуре уплаты цены сделки и не универсальный способ справедливо разрешить спор между продавцом и покупателем. Это один из самых сложных и самых спорных инструментов во всей структуре сделки.

Причина кроется в том, что earn-out не устраняет разногласия сторон по поводу стоимости бизнеса, а лишь откладывает момент их окончательного урегулирования. Спор о том, сколько стоит актив, переносится из момента сделки в будущее — в тот период, когда контроль над бизнесом уже с большой долей вероятности перешел к покупателю. В этот момент компания уже не принадлежит продавцу, но при этом право продавца на часть цены зависит не от факта совершения сделки, а от того, как этот бизнес покажет себя после закрытия, то есть после перехода к новому владельцу.

Именно поэтому earn-out требует от сторон куда большей зрелости, чем классическая модель с фиксированной ценой, так как **этот инструмент предполагает справедливое распределение риска**, а значит и качество юридической конструкции, точность финансовых определений, пределы контроля после закрытия сделки и способность сторон заранее увидеть, где именно в будущем может зародиться конфликт, и договориться о том, как его решить.

Что такое earn-out

В упрощенном виде earn-out обычно описывают как дополнительную выплату продавцу при достижении определенных показателей после сделки. На практике earn-out — это условная, **переменная часть цены, привязанная к наступлению заранее согласованных обстоятельств** или достижению бизнесом определенных результатов после перехода прав на бизнес.

Именно условность и делает этот механизм одновременно и полезным, и в некоторой степени опасным. С одной стороны, она позволяет преодолеть тупик в переговорах.

С другой — создает шлейф взаимных обязательств и потенциальных претензий уже после закрытия сделки. Если в обычной сделке стороны, как правило, расходятся после исполнения основных обязательств, то earn-out, наоборот, удерживает их в экономическом и правовом взаимодействии еще месяцы, а иногда и годы.

Поэтому earn-out нельзя назвать «бонусом продавцу» или жестом доброй воли со стороны покупателя. Это прежде всего способ поделить между сторонами риск ошибки в оценке бизнеса.

Почему earn-out появляется в сделке

Практически всегда earn-out возникает по одной и той же причине — когда **стороны по-разному смотрят на стоимость актива, но не хотят отказываться от самой сделки.**

Продавец считает, что текущая отчетность не отражает реальный потенциал бизнеса. Он видит впереди рост, новые контракты, расширение продуктовой линейки, эффект от уже сделанных инвестиций, коммерциализацию технологии, новые рынки или иные факторы, которые должны существенно повлиять на стоимость компании. Покупатель же готов платить за подтвержденный результат, но не хочет оплачивать прогноз, который пока еще не сбылся. Earn-out становится своеобразным «мостом» между этими позициями. Он позволяет покупателю зафиксировать базовую цену на уровне, который он считает защищаемым, а продавцу сохранить право на дополнительную стоимость, если его ожидания действительно реализуются.

Именно поэтому earn-out особенно востребован в сделках Tech M&A, где ценность бизнеса в значительной степени лежит в будущем. Это характерно для технологических компаний, быстрорастущих сервисов, нишевых B2B-игроков, активов с сильной зависимостью от основателя и/или команды, продукта или отдельных коммерческих этапов развития — проще говоря, для тех случаев, когда результаты прошлых периодов сами по себе не дают исчерпывающего ответа на вопрос о реальной стоимости компании.

В периоды волатильности роль earn-out существенно усиливается. Чем дороже капитал, чем осторожнее покупатели, чем сильнее недоверие к агрессивным прогнозам и чем выше давление на возвратность инвестиций, тем чаще условная часть цены оказывается единственным способом не потерять сделку на этапе согласования стоимости актива.

Какие задачи решает earn-out

Прежде всего earn-out **помогает преодолеть тупик в переговорах по цене.** Это его базовая и самая очевидная функция. Если стороны расходятся в оценке, но в остальном понимают стратегическую подоплеку сделки, earn-out позволяет перестать спорить о перспективах и связать часть цены с тем, как эти перспективы реализуются в реальности.

Но этим роль earn-out не ограничивается: его нередко используют и как **инструмент удержания вовлеченности продавца или ключевой команды** после закрытия. Для многих технологических бизнесов ценность заключена не только в активах, но и в людях — в способности основателя удерживать клиентов, собирать команду, развивать продукт, быстро принимать решения и поддерживать коммерческий темп. Формально покупатель может приобрести такой бизнес за один день, но фактически без плавной передачи дел и сохранения управленческой линии он рискует получить совсем не тот актив, за который заплатил.

В такой конфигурации earn-out становится уже не только механизмом регулирования цены, но и инструментом мотивации. Если значительная часть цены выплачивается позже и зависит от результата, продавец заинтересован не просто выйти из капитала, а помочь бизнесу пройти переходный период без негативного влияния на его стоимость.

Наконец, earn-out полезен в ситуациях, когда у компании есть убедительная история роста в ближайшем будущем, но она еще не материализовалась в тех показателях, которые покупатель готов принять как базу для оценки. Это типично для активов с сильным портфелем перспективных проектов, продуктом на стадии масштабирования или ожидаемыми регуляторными и рыночными факторами роста.

Earn-out не устраняет конфликт, а формирует путь к его разрешению

Главное, что нужно понимать сторонам с самого начала, — это то, что earn-out **не может исправить недостатки актива** или заменить due diligence, как не может и компенсировать отсутствие доверия между сторонами. Также он не является заменой гарантий и заверений и иных инструментов распределения рисков. И уж точно он не способен сам по себе превратить невыгодную сделку в выгодную.

Если у покупателя есть сомнения в качестве бизнеса, устойчивости клиентской базы, прозрачности экономики актива, надежности команды или реальности заявленного роста, earn-out не снимает эти вопросы. Он лишь откладывает их экономическое разрешение на более поздний период. В этом и состоит ключевая особенность этого инструмента: вместо спора о цене в ходе переговоров стороны получают спор о результате уже после закрытия сделки, а вместе с ним и неизбежный вопрос о том, кто именно повлиял на этот результат.

Спор почти всегда оказывается не о цифрах, а о контроле

На бумаге earn-out выглядит как финансовая формула. По существу же это почти всегда **спор о контроле над бизнесом в период после закрытия сделки.** До закрытия активом управляет продавец, после — покупатель. И именно покупатель начинает принимать решения, которые способны прямо влиять на достижение или недостижение тех показателей, от которых зависит обязанность по выплате earn-out. Он может изменить коммерческую стратегию, пересобрать команду, сократить расходы на маркетинг, в целом перераспределить расходы, встроить компанию в структуру группы, централизовать функции, изменить ассортимент, пересмотреть бюджет или отказаться от части бизнес-направлений. С точки зрения покупателя это может быть абсолютно рациональным управлением приобретенным активом. Более того, именно в этом зачастую и состоит экономическая логика сделки — интегрировать бизнес, извлечь синергии, устранить дублирование функций, перестроить модель управления. Но для продавца те же самые действия могут означать искусственное разрушение базы для earn-out.

Поэтому основной конфликт почти всегда кроется не в том, достигнут ли KPI в принципе, а в том, **почему именно KPI не был достигнут.** Бизнес действительно оказался слабее, чем заявлялось в ходе переговорного процесса, или же покупатель, уже получив контроль, повел его по иной траектории и тем самым лишил продавца шанса на получение условной части цены? Как только спор переходит в эту плоскость, становится очевидно, что earn-out — это не просто часть формулы суммы сделки, а договоренность о том, как стороны будут жить вместе после закрытия, и до какой степени покупатель вправе управлять бизнесом свободно, если его решения затрагивают право продавца на часть цены.

Дьявол в деталях

Главное заблуждение в отношении механизма earn-out состоит в том, что сторонам часто кажется, будто сначала можно договориться «в целом», а нюансы прописать позже. Но на практике именно эти нюансы и составляют весь смысл конструкции.

Первое и главное — **правильно выбрать показатель**, к достижению которого будет привязана выплата earn-out. На практике стороны любят EBITDA, потому что кажется, что этот показатель лучше отражает качество бизнеса. Но именно EBITDA часто становится самым конфликтным KPI, так как на нее влияет огромное количество факторов от учетной политики до изменения коммерческой модели. Не случайно в более широкой международной практике выручка используется как более используемая метрика для earn-out заметно чаще, чем EBITDA, так как спорить о ней обычно легче. Это не значит, что выручка всегда лучше. Иногда она, наоборот, искажает экономику: выручку можно «купить» скидками, отсрочками, убыточными контрактами или ростом некачественной дебиторской задолженности. Поэтому вопрос не в том, какой KPI более универсальный,

а в том, какой KPI действительно отражает ту ценность, за которую покупатель готов доплачивать именно в этом бизнесе.

Другая частая ошибка — согласовать общий KPI, не согласовав **реальную механику его расчета.** Стороны, например, согласовали, что earn-out выплачивается при достижении определенного уровня EBITDA. На уровне основных условий сделки / term sheet это выглядит достаточным. Но в реальной жизни EBITDA — это не просто цифра, а результат множества управленческих и иных решений: какие расходы в нее включаются, как учитываются разовые статьи, что происходит с внутригрупповыми оборотами, как отражаются инвестиции, резервы, изменения учетной политики, трансфертное ценообразование, курсовые эффекты, аллокация общегрупповых затрат и многое другое.

В этот момент становится ясно, что спор идет уже не о самом earn-out, а о том, кто и как управляет цифрой, от которой он зависит. Именно поэтому хороший KPI для earn-out — тот, который лучше всего отражает предмет сделки и при этом относительно устойчив к манипулированию. Для одного бизнеса это может быть выручка. Для другого — валовая прибыль. Для третьего — удержание ключевых клиентов, выполнение конкретного набора проектов, запуск продукта, достижение согласованных этапов развития, получение лицензии или иной объективно проверяемый результат. Выбор зависит от природы актива, но логика всегда одна: **показатель должен быть экономически связан с тем приростом стоимости бизнеса**, за который покупатель готов доплачивать, и при этом быть достаточно прозрачно проверяемым.

Как сделать earn-out рабочим инструментом

Для определения, что есть «рабочий» earn-out, сторонам нужно сначала честно ответить на вопрос **«какой риск мы пытаемся предусмотреть»** или **«какую именно ценность он должен отразить»**? Будь это рост выручки, подтверждение спроса на продукт, удержание команды или что-то иное — если стороны не могут ясно сформулировать, что именно является предметом отложенной части цены, вся конструкция изначально будет нестабильной.

Следующий шаг — это **детальная проработка методики расчета.** Формула должна быть написана так, как будто спор уже случился. Нельзя исходить из позиции «общего понимания сторонами друг друга», нужно прописывать расчет KPI так, чтобы через два года независимый консультант смог бы его воспроизвести без устных пояснений. Если это невозможно, значит, earn-out не согласован достаточно качественно.

К примеру, нельзя ограничиться фразой «earn-out выплачивается при достижении EBITDA 500 млн руб.». Нужно договориться, как именно считается EBITDA: по каким стандартам, с какими корректировками, как учитываются разовые доходы и расходы, курсовые разницы, внутригрупповые обороты, изменение учетной политики, M&A внутри группы покупателя, влияние синергий, трансфертное ценообразование, новые инвестиции и так далее. Практикующие M&A-специалисты всегда согласятся с тем, что согласование учетной политики еще на стадии ДКП резко снижает риск будущих конфликтов.

Не менее важно **согласовать принципы корпоративного управления** после закрытия сделки. Покупатель должен понимать, какие действия после закрытия он вправе предпринимать свободно, а какие могут повлиять на earn-out. Продавец, в свою очередь, должен

понимать, в какой степени он защищен от того, что новая стратегия, интеграция, перераспределение функций или смена менеджмента будут давить на согласованный KPI. Чем меньше в этом вопросе стороны полагаются на добросовестность друг друга и чем больше конкретных правил заложено в договор, тем выше стабильность всей конструкции.

Отдельно должны быть урегулированы **информационные права продавца.** Если earn-out зависит от результатов бизнеса, продавец должен иметь возможность проверить корректность расчета, получить доступ к определенному объему отчетности, заявить возражения, при необходимости инициировать экспертную проверку. Иначе право на earn-out быстро превращается в право спорить вслепую.

Наконец, необходимо заранее определить **механику разрешения разногласий.** Кто и как проверяет KPI, в каком объеме, где заканчивается расчет и начинается спор о добросовестности поведения покупателя, что происходит при частичном выполнении показателя и др. Эти вопросы не всегда приятны в ходе переговоров, но именно они решают, будет ли earn-out работать в реальной жизни.

Также не стоит забывать и о сугубо практичных аспектах предполагаемого платежа — нужна **четко согласованная платежная и обеспечительная механика:** срок выплаты, валюта, источник платежа, проценты за просрочку, использование счета эскроу, банковская гарантия, залог, право удержания части суммы, факторы досрочной выплаты или утраты права на нее и пр.

Основные риски earn-out

(1) Манипулируемость показателем

Если KPI зависит от воли покупателя, продавец экономически становится заложником чужого управления. Это особенно опасно, когда после сделки бизнес интегрируется в большую группу: меняются каналы продаж, перераспределяются расходы, переводятся сотрудники, перезаключаются договоры, меняются принципы признания выручки. Формально бизнес может продолжать работать, но база для earn-out уже будет размыта.

(2) Конфликт между интересами интеграции бизнеса и интересами продавца

Для покупателя может быть рационально быстро встроить актив в свою группу, объединить функции, изменить ассортимент, пересмотреть клиентскую политику, закрыть часть направлений. Для продавца это может означать потерю шанса на earn-out. С этого момента спор будет вестись уже не о формуле, а о том, должен ли покупатель управлять активом в интересах своей группы или в интересах выполнения earn-out. Именно в этой области рождается большая часть конфликтов после закрытия сделки.

(3) Временной горизонт

Чем длиннее период выплаты earn-out, тем выше вероятность, что на результат повлияют не только усилия сторон, но и внешний рынок: ставка, курс, регулирование, поведение клиентов, санкции, изменение цепочек поставок, налоговые правила и пр. В этот момент начинается спор, не выполнен ли KPI из-за качества бизнеса или же из-за внешних шоков. Если этот вопрос не решен в договоре, то конфликт почти неизбежен.

(4) Смешение цены и ответственности

На переговорах earn-out иногда используют как некий суррогат механизма гарантий — если что-то пойдет не так, earn-out не будет выплачен. Так это работать не должно. Earn-out — это инструмент цены, а не замена заверений, гарантий, возмещения потерь или иных специальных механизмов. Если смешать эти понятия, сделка становится внутренне противоречивой.

(5) Налоговые и корпоративные эффекты

Отложенная и условная часть цены **должна** быть корректно «вшита» в договорную и платежную механику, иначе стороны сталкиваются с вопросами документального подтверждения, момента возникновения обязательства, валюты расчета, обеспечений, компетенций органов управления, а также с технической возможностью реализовать второй этап выплаты цены или передачи актива.

Российский контекст: почему особенно важны юридические и корпоративные аспекты

Для российского рынка M&A earn-out сам по себе уже давно не является экзотикой. Но именно на российском рынке особенно хорошо видно, что экономическая идея без качественного юридического и корпоративного структурирования не работает.

Недостаточно зафиксировать общую мысль о том, что при достижении определенного результата покупатель доплачивает продавцу. Нужно, чтобы условная часть цены была определима, порядок расчета — воспроизводим, корпоративные шаги — технически исполнимы, а возможный спор — доказуем. Это особенно важно в сделках с долями в ООО, в многоэтапных структурах, в конструкциях с опционами, где earn-out влияет не только на окончательную цену, но и на дальнейшее перераспределение корпоративных прав.

В таких случаях ошибка в механике уже не только создает почву для спора о сумме платежа, но способна поставить под вопрос исполнимость всей структуры сделки. Поэтому в российских реалиях чем точнее конструкция «собрана» на финансовом, договорном и корпоративном уровнях, тем выше шанс, что она будет работать по назначению. Чем больше в ней общих формулировок и недосказанности, тем выше вероятность, что она станет причиной долгого и дорогого конфликта.

Заключение

Earn-out — это, безусловно, крайне полезный инструмент, а зачастую и единственный способ сохранить сделку, особенно в условиях высокой волатильности и дорогого капитала. В правильной конфигурации он действительно помогает закрывать сделки, которые иначе развалились бы на этапе согласования цены. Он позволяет примирить разные взгляды на стоимость бизнеса, распределить риски, сохранить мотивацию продавца в переходный период и связать часть цены с реальным подтверждением заявленного роста. Но у этого инструмента есть одна важная особенность — он не работает на общих словах о партнерстве и разумности и не защищает, если договоренности были о принципе, а детали оставили на потом.

По-настоящему качественно проработанный earn-out — это тщательно собранный механизм, в котором стороны заранее ответили на все неприятные вопросы: что именно должно быть достигнуто, как это считается, кто влияет на результат, какие действия после закрытия допустимы, а какие — нет, и что произойдет, если через год каждая сторона будет уверена, что именно она права.

Главное, что необходимо понимать, это то, что earn-out — это не способ уйти от спора о цене. Это способ постараться очень точно распределить риск между сторонами. Если такая точность достигнута, он действительно работает. Если нет — он не спасет сделку, а просто перенесет конфликт в будущее, где цена ошибки почти всегда будет выше.

2 Due Diligence и управление рисками в сделках Tech M&A



Раздел 1

Области проверки и ключевые риски IT-компаний

АВТОРЫ



Анастасия Нерчинская



Александр Панов
VERBA LEGAL



Роман Головацкий
DENUO

Краткие выводы

- Приоритетные области проверки конкретного IT-бизнеса зависят от множества факторов — отраслевой специфики компании, ее бизнес-модели и сегмента рынка, объема применимых регуляторных требований, этапа жизненного цикла компании и стратегических целей инвестора. Стандартного подхода не существует.

- В большинстве IT-компаний ключевыми областями проверки являются: (i) «чистота» титула на ключевое ПО в составе продукта; (ii) вопросы мотивации технической команды; (iii) отношения с конечными потребителями. Это — условная «программа-минимум» due diligence IT-бизнеса в контексте сделки M&A.

- В 2025 г. инвесторы стали больше внимания уделять проверке юридической «чистоты» прав на ключевое ПО. Это обусловлено тем, что для многих IT-компаний ПО является основным внеоборотным активом, лежащим в основе стоимости бизнеса. Важнейшей предпосылкой оценки является наличие титула на все ключевые активы, напрямую «участвующие» в создании стоимости IT-компании. На фоне низких мультипликаторов оценки в 2025 г. наличие рисков в отношении ключевых активов приобретаемой компании могло ухудшить позицию продавца.

- В связи с завершением в 2025 г. действия моратория на проведение проверок в отношении аккредитованных IT-компаний в 2026 г. со стороны надзорных органов продолжится активность, в первую очередь, по таким направлениям, как антимонопольный комплаенс (особенно для компаний с крупной долей рынка), правомерность применения налоговых льгот, а также соблюдение требований по защите ПДн.

- В 2025 г. было ужесточено регулирование сферы ПДн, отмечен кратный рост штрафов и внедрена автоматизированная система мониторинга Роскомнадзора. Риски, связанные с нарушением требований текущего регулирования ПДн, потребовали более глубокого анализа, чем проведение формальной проверки.

- В Tech M&A проектах формата asset-deal наличие дефектов титула на ключевое ПО является критичным риском. Такая ситуация препятствует передаче покупателю прав на продукт и, как следствие, получению контроля над ним. Поэтому, в отличие от формата share-deal, такая структура требует особого внимания к юридической «чистоте» прав на ключевое ПО.

- При оптимизации due diligence важно не сокращать объем проверки до формального уровня. Поверхностный анализ (например, оценка только последнего звена цепочки передачи прав или ограничение проверки титула сведениями из реестра Роспатента) не позволит выявить критические дефекты титула на ключевой актив.

- Часть рисков, связанных с дефектами титула на ПО, в зрелых IT-бизнесах не поддается эффективному устранению по причине «откладывания» урегулирования этих вопросов на поздние стадии. Это, в свою очередь, существенно влияет на сроки и возможность реализации сделки, а также на ее структуру.

- Среди наиболее распространенных рисков (ТОП-5), выявляемых по итогам due diligence IT-компаний, участники опроса отметили: (i) отсутствие титула на ключевое ПО; (ii) предъявление требований о выплате авторского вознаграждения; (iii) увольнение IT-команды после закрытия сделки; (iv) утрата компанией IT-льгот; (v) отсутствие контроля за экземпляром кодовой базы. Все указанные риски, за исключением требований выплаты авторского вознаграждения и утраты IT-льгот, респонденты опроса также отметили как наиболее критичные, способные существенно повлиять на структуру сделки и ее условия.

1.1 Ключевые области и направления due diligence IT-компаний

Правильное определение круга ключевых аспектов анализа — первый шаг к эффективной юридической проверке IT-компании. Далеко не все вопросы, требующие внимательного изучения в рамках деятельности одной компании, будут столь же актуальными при проверке другой. Какие аспекты деятельности конкретной компании следует изучить в приоритетном порядке, а что можно вывести за периметр проверки, определяется в каждой ситуации индивидуально и зависит от множества факторов. Единого стандарта и универсальной методологии не существует.

Что следует учесть при определении областей проверки IT-компании

Чтобы определить приоритетные области due diligence IT-компании, важно оценить влияние на ее деятельность следующих факторов:

- отраслевая специфика компании, вертикаль и сегмент рынка (B2B / B2C / B2G и т. п.);
- оценка (EV) и масштаб бизнеса;
- объем применимых к компании регуляторных требований (например, сертификация или лицензирование);
- бизнес-модель компании, специфика, определяемая типом продукта (например, enterprise software, облачный сервис, телеком-оператор, системный интегратор, производитель программно-аппаратных комплексов или оператор ИИ-системы);
- стратегические цели покупателя, его намерение интегрировать приобретаемый актив в собственные IT-контур и бизнес-модель, а также участвовать в его операционном управлении и развитии;
- параметры сделки, включая фактор срочности и тип M&A-процесса (конкурентный или эксклюзивный);

- стадия жизненного цикла компании, степень зрелости ее продукта;
- качество внутренних процессов разработки и управления данными;
- объем ресурсов и времени, которыми располагает покупатель для проведения аудита.

Таким образом, приоритеты due diligence IT-компании всегда адаптируются под конкретный кейс с учетом бизнес-задач и особенностей приобретаемого актива.

#ОБЛАСТИ_DUE_DILIGENCE



Екатерина Абясова

старший юрист практики корпоративного права / слияний и поглощений

Melling Voitishkin &Partners

Определение приоритетных областей для проверки бизнеса обусловлено спецификой отрасли, в которой таргет осуществляет свою деятельность.

Для компаний телекоммуникационного сектора, в первую очередь, анализу подлежат:

- Соблюдение регуляторных требований: лицензии, иные разрешения (например, использование радиочастотного спектра), выполнение условий эксплуатации сетей и телеком-оборудования и т. д.
- Права таргета на ключевые активы, включая сеть связи и оборудование.
- Договорная обвязка модели оказания услуг, способы сохранения клиентской базы и обеспечения непрерывности ведения бизнеса после продажи (особенно в случае, когда часть клиентов обслуживается по глобальным договорам с продавцами).
- Финансовое положение таргета и вопросы урегулирования внутригрупповой задолженности до закрытия сделки.

Для IT-компаний ключевыми областями проверки являются:

- права таргета на базы данных и ПО;
- права таргета на используемые сайты, домены, аккаунты и прочие онлайн-активы;
- пользовательская база и варианты ее сохранения после продажи;
- ИТ-инфраструктура и риски ее потери после смены контроля.

Проверка ключевых активов — «программа-минимум»

Традиционно областью первого приоритета юридической проверки являются аспекты, связанные **с ключевыми активами**, от которых напрямую зависит стоимость бизнеса. Риски, связанные с дефектами таких активов, не выявленные до закрытия сделки, впоследствии могут дорого обойтись приобретателю компании.

В абсолютном большинстве IT-бизнесов к ключевым активам относятся:

- программное обеспечение;
- интеллектуальный капитал — команда разработки и технической поддержки;
- клиентская база и потенциальный объем рынка.

Особенностью due diligence IT-компаний является то обстоятельство, что многие значимые активы «скрыты от глаз» и сложны для анализа в рамках документарного подхода. Часть из них не имеет осязаемой (овеществленной) формы, сложна в оценке в отрыве от бизнеса в целом, а некоторые не являются активами в буквальном смысле слова (например, команда, интеллектуальный капитал и навыки, доверие клиентов, качество бизнес-процессов и т. п.). Однако именно эти активы, наряду с ПО, являются основными в абсолютном большинстве IT-бизнесов.

Потому для правильной правовой квалификации вопросов, связанных с ключевыми IT-активами, важным подспорьем могут оказаться **выводы технической экспертизы** или, как минимум, ответы, полученные в ходе **интервью технической команды** приобретаемой компании.

#РЕЗУЛЬТАТЫ_ОПРОСОВ



Считают, что в 2025 г. инвесторы стали больше внимания уделять проверке и митигации рисков, связанных с титулом на ПО

По данным Опроса по аспектам Tech M&A.

ПО — один из самых сложных объектов правового анализа. Чтобы не увязнуть в деталях, важно четко определить: (i) какое ПО («версия» продукта) на текущий момент находится на продакшен-сервере; (ii) какие части кодовой базы, размещенные в различных средах, ему соответствуют; (iii) где находятся и кто контролирует все предыдущие «версии» продукта (это значимый актив, который также должен быть включен в периметр проверки несмотря на его кажущуюся «вторичность»); (iv) существует ли техническая документация к ПО и в каком формате. Также важна функциональная (ключевые модули и подсистемы) и коммерческая (например, в разрезе выручки) детализация архитектуры продукта.

Наличие этих данных позволяет выделить главные области проверки ключевого ПО.

Очень условно можно сказать, что для продуктовой компании B2B-сегмента минимальный объем юридической проверки — права на текущую «версию» продукта, размещенную на продакшен-сервере.

Вопросы «второго плана»

Второстепенными, но также значимыми аспектами деятельности IT-компаний являются зрелость ее бизнес-процессов, IT-комплаенс (системы мониторинга и управления метриками развития продукта), возможность применения льгот и спецрежимов, необходимость импортозамещения, наличие доступа к массивам данных, устойчивые связи с поставщиками ключевых ресурсов, инфраструктура.

Так, для многих IT-компаний, особенно молодых, важным является **вопрос льгот и преференций**. Поэтому в рамках due diligence большое внимание уделяется аспектам аккредитации IT-компаний, правомерности применения соответствующих налоговых и регуляторных преимуществ и оценки рисков их утраты.

Практически для всех компаний, работающих в сегменте B2C, особое значение имеет **соблюдение регуляторных требований в сфере ПДн**. При приобретении поставщика IT-решений для публичного сектора особенно важно проверить соблюдение **требований импортозамещения, режимов лицензирования, санкционных ограничений**.

#РЕЗУЛЬТАТЫ_ОПРОСОВ



Стали больше внимания уделять проверке регуляторных вопросов, включая вопросы импортозамещения



Стали больше внимания уделять проверке рисков, связанных с налоговыми льготами и преференциями для IT-компаний

По данным Опроса по структурированию сделок Tech M&A в 2025 г.

Почти в каждом продуктовом бизнесе значимыми являются вопросы юридической «чистоты» **использования open source компонентов** и совместимости лицензий.

Если же компания имеет высокую **концентрацию выручки / контрактов** — в рамках юридической проверки следует уделить особое внимание соответствующим договорам и их специфическим условиям, прежде всего, о сроке действия и основаниях выхода контрагента из договора.

В ряде случаев важное имеют значение и **иные вопросы**, в том числе относящиеся к смежным областям регулирования, помимо IP / IT.

Например:

- брендирование продуктовой линейки и правомерность использования товарных знаков и иных логотипов;
- специфика применения отдельных технологий (блокчейн, IoT, ИИ и робототехника и т. п.);
- функционирование ЦОДов и других объектов IT-инфраструктуры;
- использование компанией интернет-сайтов, различных информационных систем, администрирование доменных имен;
- сертификация, лицензирование, аттестация, включение в реестры, иные вопросы государственного контроля в зависимости от отраслевой специфики IT-компании;
- права на иные ОИС, например, дизайн, брендбуки, чертежи и т. п.;
- вопросы трудового и миграционного права, не связанные с анализом круга должностных обязанностей разработчиков (режимы дистанционной работы программистов, работа из-за рубежа и т. п.);
- антимонопольные вопросы.

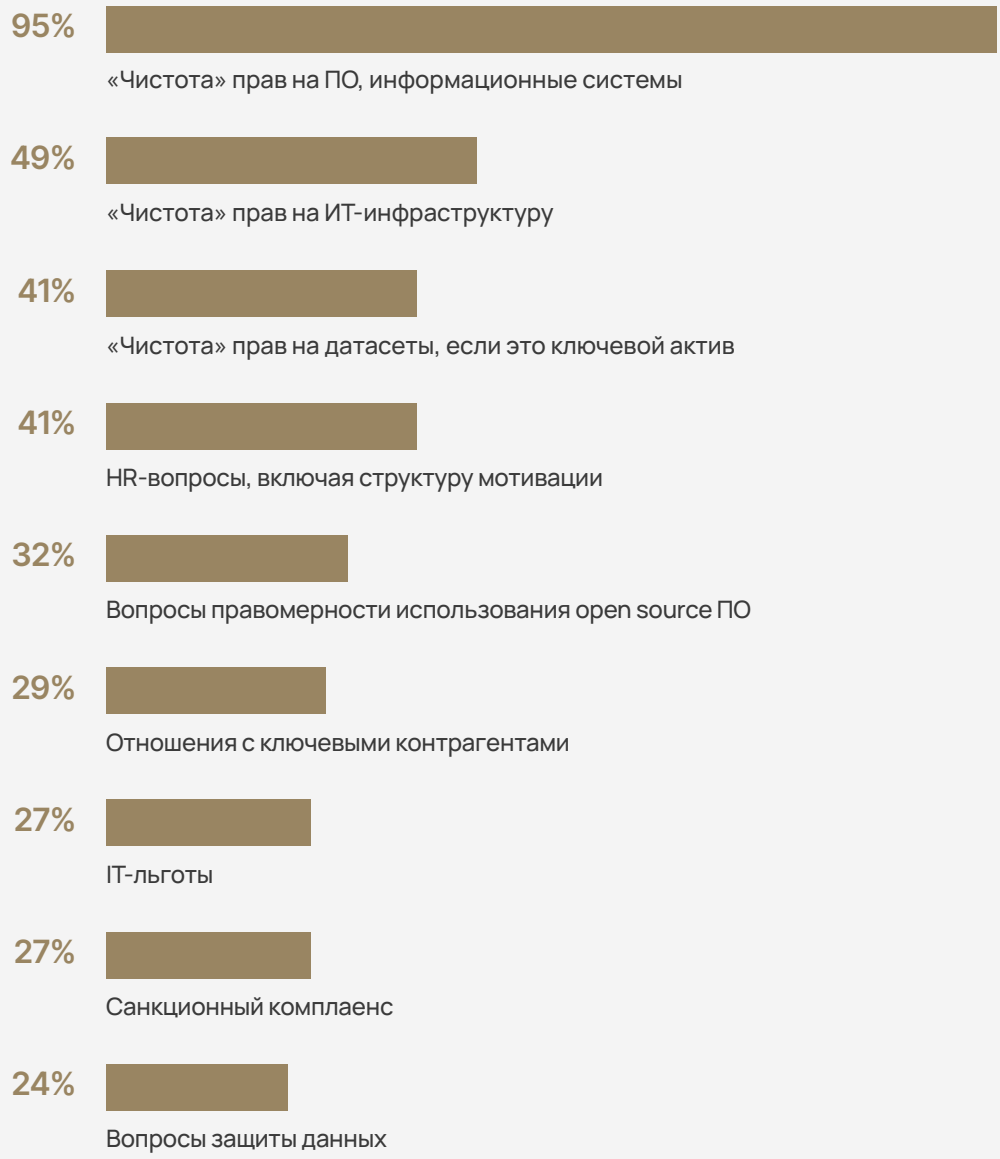
Прежде чем составить план проверки IT-компании, важно учесть указанные выше факторы, отсечь то, что не применимо, и сосредоточиться на принципиально значимых вопросах.

> **Приоритеты due diligence IT-компании всегда адаптируются под конкретный кейс с учетом бизнес-задач и особенностей приобретаемого актива. Единого стандарта проверки, как и универсального чек-листа с запросом информации для проверки, не существует. Даже бизнесы одного типа могут иметь существенные отличия как в активах, так и по характеру рисков. Любой стандартизированный формат юридической проверки — лишь поверхностный взгляд на задачу, не учитывающий специфику данного бизнеса.**

В ходе исследования мы провели опрос, в рамках которого попросили респондентов отметить **ключевые, по их мнению, области проверки IT-компаний**.

#РЕЗУЛЬТАТЫ_ОПРОСОВ

Какие области проверки due diligence ИТ-компании являются, на ваш взгляд, наиболее важными и приоритетными?



По данным Опроса по аспектам Tech M&A (41 респондент).

#ОБЛАСТИ_DUE_DILIGENCE



Роман Головацкий

партнер

dénuo

Вопрос приоритетности того или иного сегмента в ходе юридической проверки зависит, в первую очередь, от специфики бизнеса и особенностей ключевых активов. Безусловно, вопрос прав и титула на ключевой актив всегда имеет важное значение, что, собственно, подтверждается результатами опроса. Между тем, например, если бизнес опирается на обработку существенных массивов персональных данных, проверка рисков в части соответствующего комплаенса будет одной из основных. Если функционирование бизнеса завязано на использовании интеллектуальных прав и сервисов третьих лиц, которые «жизненно» необходимы для нормальной работы бизнеса, то, очевидно, что проверка взаимоотношений с контрагентом, достаточности объема полученных от него лицензий также будет носить определяющий характер.

Как показали итоги опроса, **безусловным лидером** среди направлений юридической проверки IT-компаний оказались **вопросы «чистоты» прав на ПО и информационные системы компании**. Это отметили **95% респондентов**. Данный вопрос особенно актуален для продуктовых компаний, где ПО — лежит в основе бизнеса.

К ним относятся:

- анализ и подтверждение всей цепочки прав на ПО от первоначального автора до конечного правообладателя, которым, предположительно, должна оказаться приобретаемая компания;
- проверка оснований утраты прав на ПО и возможности его использования в будущем, а также физического контроля кодовой базой;
- оценка рисков финансовых санкций, связанных с неправомерным использованием ПО;
- проверка оснований для предъявления претензий авторами ПО в связи с нарушением их личных неимущественных прав, а также права на получение вознаграждения;
- анализ рисков претензий от контрагентов компании в связи с возможным простоем бизнеса, временной невозможностью оказания услуг или нарушением гарантий наличия титула на ПО

и ряд других[7].

С заметным отрывом по числу голосов (**49% респондентов**) среди приоритетов due diligence следуют вопросы «чистоты» прав на IT-инфраструктуру. При оценке значимости инфраструктурных вопросов важно понимать намерения покупателя по **интеграции актива** в свой контур, сроков ее поведения и **планов по масштабированию**. Если предполагается интеграция с системами покупателя, важно проанализировать вопросы инфраструктуры с учетом позиции технической команды о допустимости интеграции и ее «бесшовности», синхронизации режимов старой и новой команды техподдержки и т. п.

Если же приобретаемая компания является **сервисным оператором инфраструктуры**, например, предоставляет услуги PaaS / IaaS, то вопросы прав на IT- и телеком-оборудование будут являться ключевым направлением юридической проверки.

[7] Более подробно вопросы, связанные с проблематикой и лучшими рыночными практиками проверки прав на ПО см. в главе 2 разделе 3 исследования.

> **Практически в каждой IT-компании к приоритетным областям проверки можно отнести: (i) ключевое ПО в составе продукта; (ii) вопросы мотивации технической команды; (iii) структуру отношений с конечными потребителями. По этим направлениям обычно выстраивается «программа-минимум» юридической проверки.**

Также к значимым областям проверки IT-компаний респонденты отнесли вопросы, связанные с использованием массивов данных и мотивацией IT-команды (**41% респондентов** в каждом случае соответственно).

Вопрос «чистоты» прав на крупные массивы данных является крайне сложным, поскольку возможность его объективного и полноценного юридического анализа вызывает сомнения. Однако если в бизнесе приобретаемой компании активно используются **технологии больших данных**, проверка этих аспектов также становится приоритетным направлением due diligence.

Анализ рисков, связанных с **возможным увольнением команды**, всегда являлся вопросом высокого приоритета. В этом случае инструментарий юридической проверки также ограничен. Однако если компания не планирует внедрять или усиливать программу мотивации ключевого персонала, это само по себе может считаться неблагоприятным коммерческим фактором.

По данным опроса, остальные области due diligence, такие как комплаенс open source, отношения с ключевыми поставщиками и заказчиками, налоговые и регуляторные аспекты (включая IT-льготы, санкционные вопросы и защиту данных), были отмечены участниками опроса как менее значимые в контексте предстоящей сделки M&A. Тем не менее, довольно существенная доля респондентов (**от 24% до 32%**) в рамках юридической проверки уделяет внимание также и этим вопросам.

#ОБЛАСТИ_DUE_DILIGENCE



Сергей Колобов

советник

NIKOLSKAYA consulting

Важной особенностью процедуры due diligence в рамках сделок Tech M&A является детальный аудит кода ПО и баз данных. Это стало особенно актуально в последние годы в связи с уходом западных компаний и предоставляемых ими решений с российского рынка, когда такие решения стали заменяться либо open source-решениями, либо собственными разработками. В обоих случаях особенно важно убедиться в отсутствии существенных рисков предъявления требований третьими лицами (включая сотрудников таргета, участвовавших в создании ПО или баз данных). Существенное использование open source требует пристального внимания, так как может представлять титульный риск для проприетарного продукта и вести к обязанности раскрытия кода такого продукта. Тем не менее, сторонам важно трезво оценивать возможность проведения анализа кода на использование open source, так как такой аудит довольно трудозатратен и зачастую невозможен с учетом сроков сделки. В таких обстоятельствах более удачным решением может быть согласование сторонами компромиссных формулировок заверений, которые, с одной стороны, закроют существенные риски для покупателя, с другой стороны, не потребуют от продавца трудоемких внутренних проверок продуктов.

#ОБЛАСТИ_DUE_DILIGENCE



Софья Смирнова

советник M&A
и корпоративной практики

O2 консалтинг

Представляется, что, помимо титула на ключевой актив в виде ПО, важно разобраться, что еще представляет собой коммерческую ценность актива, и детально проанализировать юридические предпосылки для утраты права на это «что-то». Чаще всего таким активом является команда, а именно ключевые сотрудники. Традиционно в юридических проверках внимание уделяется лишь вопросам их компенсации, наличию опционных и мотивационных программ и их условия. Вместе с тем пока не сложилось однозначной рыночной практики проводить беседу между ключевыми сотрудниками и юристами, проверяющими актив, для выяснения юридически значимых обстоятельств нахождения данных лиц в коллективе, основаниях их лояльности текущему руководству. Потеря ценных кадров может повлечь гораздо большее понижение стоимости актива, чем может увидеться в сухих расчетах финансовых показателей, и нести риск их недостижения так или иначе придется не только продавцу (в случае с earn-out), но и покупателю, лишившемуся значительной части стоимости актива и не предпринявшему мер разумной осмотрительности для предотвращения данной ситуации до входа в сделку.

#ОБЛАСТИ_DUE_DILIGENCE



Илья Булгаков

советник

dénuo

Результаты опроса в принципе предсказуемы: на первых трех местах расположилась триада — права на программное обеспечение, инфраструктура и датасет. Отмечу лишь, что, в зависимости от индустрии таргета, значимость отдельных позиций может меняться с точки зрения важности. Например, если бизнес построен на интеграции или на локализации и дистрибуции онлайн-игр сторонних разработчиков, то особое значение будут иметь отношения с ключевыми клиентами и лицензионные соглашения с разработчиком игр. В консьюмерских бизнесах особое значение всегда имеет вопрос соблюдения законодательства о персональных данных (программы лояльности, получение данных для маркетинговых рассылок, пользовательские данные).

#ОБЛАСТИ_DUE_DILIGENCE



Анастасия Духина

старший юрист практики корпоративного права / M&A

sll

В юридическом due diligence ИТ-компаний основное внимание уделяется, безусловно, оформлению прав на основные объекты интеллектуальной собственности (как собственные разработки, так и лицензии), регулированию отношений с ключевыми работниками, а также коммерческим вопросам, способным негативно сказаться на деятельности компании. Например, в одной из сопровождаемых нами сделок большое значение имели не только сами разработки таргета, но и действительность договоров аренды помещений, где располагаются основные производственные мощности и внезапная утрата которых вполне может остановить деятельность таргета на неопределенный срок.

#ОБЛАСТИ_DUE_DILIGENCE



Антон Назаренко

старший юрист
практики интеллектуальной
собственности

Melling Voitishkin &Partners

Due diligence не ограничивается лишь проверкой титула на ПО. Так, разработка ПО начинается не с кода, а с работы, например, системных аналитиков, которые разрабатывают архитектуру ПО. Кроме того, при проведении due diligence Tech компаний, особенно в B2C-сегменте, необходимо также проверить, защищены ли логотипы и наименования продуктов в качестве товарных знаков. Нередко разработка сопутствующих материалов (например, маркетинговых) поручается внешним исполнителям, однако в договорах подряда или оказания услуг не всегда содержатся положения о передаче исключительных прав на созданные РИД.

#ОБЛАСТИ_DUE_DILIGENCE



Владислав Лазуткин

старший юрист

ORION

При проверке бизнесов в сегменте B2B Software можно отметить два фактора: (i) трансграничную фрагментацию бизнеса таргета — один и тот же продукт (ПО) может продаваться и российским, и иностранным клиентам под разными брендами / с использованием внешне независимых структур; (ii) большое внимание к крупным контрактам — ввиду ограниченного эффекта от импульса на импортозамещение многие провайдеры ПО для бизнеса остаются зависимы от небольшого ряда крупных контрактов / клиентов.

#ОБЛАСТИ_DUE_DILIGENCE



Бесханум Мамедова

консультант практики цифрового права и интеллектуальной собственности

o2 consulting

Согласно новым правилам, введенным Постановлением Правительства РФ № 1949 от 26.12.2025 г., для получения и сохранения аккредитации ИТ-компания должна находиться под российским контролем. Так, в соответствии с новыми требованиями в отношении непубличных обществ, более 50% владения должно принадлежать российским субъектам, публичные общества не должны находиться под иностранным контролем.

Факт несоответствия новым требованиям является основанием для прекращения действия аккредитации в процессе ее ежегодного подтверждения, которое должно быть завершено не позднее 1 июля.

Оптимизация объема due diligence

Нередко «серийные» приобретатели IT-активов пытаются оптимизировать периметр юридической проверки IT-бизнесов, исключая ряд вопросов, которые, по их мнению, не будут иметь существенного влияния на сделку в целом. Основной причиной является традиционная проблема нехватки времени и ресурсов на проведение полноценной проверки.

В ходе исследования мы попросили респондентов онлайн-опроса отметить, каким областям due diligence IT-бизнеса, по их мнению, можно уделить второстепенное значение или вообще вывести за рамки анализа.

#РЕЗУЛЬТАТЫ_ОПРОСОВ

Какие аспекты вы без особой причины не будете включать в периметр юридического due diligence при приобретении IT-компании?



По данным Опроса по аспектам Tech M&A (41 респондент).

54% респондентов отметили, что вряд ли будут уделять большое внимание проверке **второстепенных программных компонентов** (тех, которые не оказывают существенного влияния на бизнес). С одной стороны, это подход выглядит разумным. Ведь наиболее серьезный риск, который может материализоваться в отношении

ПО, — это **запрет его использования компанией на будущее время**. Если ПО не является ключевым — риск его утраты обычно не оценивается как высокий.

Однако при использовании такого подхода **следует быть очень внимательными при определении перечня наиболее значимых компонентов ПО**, которыми планируется ограничить периметр проверки. Этот вопрос носит исключительно оценочный характер. При этом юристы, в том числе юридическая инхаус-команда приобретаемой компании, не может самостоятельно установить степень значимости различных компонентов продукта. В данном случае **такая позиция требует обоснования технической, финансовой и операционной команд** компании и покупателя.

> **IT-активы не имеют осязаемой (овеществленной) формы, их сложно правильно оценить в отрыве от бизнеса в целом, некоторые из них не являются активами в буквальном смысле слова (например, команда, интеллектуальный капитал и навыки, доверие клиентов, качество бизнес-процессов и т. п.). Однако именно эти объекты, наряду с ПО, являются ключевыми в большинстве IT-бизнесов и формируют их ценность.**

44% респондентов ответили, что не будут включать в объем проверки титул на ПО, депонированное в Роспатенте. Однако **такое ограничение может повлечь серьезные правовые риски**. Государственная регистрация ПО носит сугубо заявительный (декларативный) характер. В отличие от регистрации товарных знаков или получения патентов, она **не гарантирует держателю свидетельства наличие титула на ПО**. По сути, в данном случае патентное ведомство лишь фиксирует факт обращения лица, которое заявляет о себе как о правообладателе. Роспатент не производит экспертизу по существу таких сведений, в том числе не проверяет, на каком основании заявитель приобрел титул.

Безусловно, наличие свидетельства о регистрации создает презумпцию правообладания, которая судами будет признаваться до момента ее опровержения. Вместе с тем такое свидетельство не является неоспоримым доказательством обладания исключительным правом и само по себе не гарантирует защиту от претензий третьих лиц. При этом если, например, компания-таргет приобретала ПО через цепочку передачи прав и в каком-то из звеньев этой цепочки имелся правовой дефект, то регистрация ПО в Роспатенте не сможет его устранить. В последнем случае, даже при наличии свидетельства о государственной регистрации, компания не будет являться фактическим правообладателем. Таким образом, ограничение юридической проверки оценкой только факта регистрации ПО в Роспатенте **не выглядит разумным подходом**.

Итоги интервью с участниками сделок Tech M&A и результаты опросов, проведенных в ходе исследования, показали, что в 2025 г. инвесторы стали больше внимания уделять вопросу юридической проверки «чистоты» прав на ПО и чаще использовать IT-специфические договорные инструменты, такие как заверения и возмещение имущественных потерь, связанные с техническими характеристиками продукта.

41% респондентов готовы исключить из периметра юридической проверки вопросы титула на ПО, которое компания-таргет приобрела по договору об отчуждении исключительного права, где указана в качестве приобретателя. На первый взгляд, такой подход выглядит обоснованным, учитывая, что в рамках проверки у юристов будут первичные документы, подтверждающие переход титула к компании. Кроме того, в судебной практике в делах о защите исключительных прав допускается в качестве подтверждения титула представление договора, в котором истец указан приобретателем. Считается, что это достаточное доказательство наличия титула, пока не будет доказано иное. Однако применение такого подхода в рамках due diligence **сопряжено с серьезной опасностью**, поскольку переход исключительного права может быть опровергнут.

Чтобы подтвердить фактический переход титула к компании, требуется проверка **всей цепочки прав, начиная с момента создания продукта**. Как уже отмечалось выше, наличие дефекта в любом из звеньев этой цепочки означает, что исключительное право могло не перейти к таргету в полном объеме либо вовсе. Соответственно, если ограничиться анализом только последнего звена передачи титула, такой подход может оказаться оценкой лишь «вершины айсберга» и привести к недооценке существенных правовых рисков отсутствия титула.

29% респондентов отметили, что ограничили бы анализ ЛНА приобретаемой компании положениями, устанавливающими должностные обязанности разработчиков ПО. Действительно, такие обязанности могут содержаться в типовой должностной инструкции, утвержденной в качестве ЛНА. Однако в рамках юридической проверки IT-компании круг значимых вопросов, покрываемых различными ЛНА, гораздо шире. Локальные акты **формируют структурную основу (фрейм) взаимодействия работников и компании в процессе разработки и развития продукта.**

К аспектам, которые обычно регламентируются на уровне ЛНА, относятся: (i) общий порядок создания в компании служебных произведений; (ii) порядок использования при создании продукта трекинговых систем, таск-менеджеров, систем контроля версий ПО, репозиториев и других информационных ресурсов и инфраструктуры, включая вопросы использования учетных записей и разграничения доступа к соответствующим объектам; (iii) процедура уведом-

ления компании о создании ПО или отдельных артефактов, а также их передачи в распоряжение компании; (iv) вопросы авторского вознаграждения за создание продукта; (v) система мотивации команды и многие другие, которые могут оказать большое влияние на общие итоги проверки.

Почти четверть респондентов (**24%**) отметили, что исключили бы из периметра проверки массивы данных, используемые приобретаемой компанией. Как отмечалось выше, юридический анализ крупных датасетов имеет серьезные ограничения. В данную область проверки обычно входят вопросы наличия у компании титула на такой датасет (например, смежного права), а также его юридической «чистоты».

Первый вопрос — это скорее предмет технической экспертизы и оценки. Один лишь юридический инструментарий не позволяет достоверно определить наличие презумпции существенности затрат на создание такого датасета. В отношении второго вопроса пока не сформировалась эффективная методология юридической проверки. Использование крупных датасетов традиционно сопряжено с триадой потенциальных рисков частно-правового и регуляторного характера: возможным нарушением прав на ОИС, незаконным использованием ПДн и информации ограниченного доступа. Из-за очень большого объема данных проверить наличие законного основания использования каждого самостоятельного информационного элемента невозможно. Метод экстраполяции здесь не будет эффективным, поскольку даже единичное нарушение, доля которого может составлять микропроцент на общем фоне, может стать основанием для взыскания штрафа или компенсации.

Тем не менее, представляется, что вопросы датасетов также следует включать в периметр юридической проверки, если они являются **ключевыми активами компании** (например, ИИ-бизнес) или деятельность компаний связана **с постоянным сбором и накоплением данных** (маркетплейсы, классифайды и т. п.), в том числе в качестве «побочного продукта». Именно так, по данным ранее приведенного опроса[8] поступили бы **41% респондентов** .

[8] См. результаты опроса на стр. 173.



Роман Головацкий

партнер

DÉNUO

Когда сроки и ресурсы на проведение юридической проверки ограничены, возникает крайне болезненный вопрос, чем жертвовать, чтобы сохранить эффективность исследования и не пропустить критические риски. В этой связи нередко за периметр проверки выносят наименее значимые для бизнеса компоненты ПО, исходя из той предпосылки, что в случае материализации рисков такие компоненты будет проще исключить или заменить. Однако существенной проблемой здесь является должная идентификация и релевантное разделение компонентного состава продукта, поэтому без связки с технической экспертизой и бизнес-командой здесь не обойтись.

Между тем на практике встречаются и случаи, когда из объема проверки необоснованно исключаются действительно существенные вопросы.

Например, если программа для ЭВМ зарегистрирована в Роспатенте, нередко можно встретить мнение, что в таком случае проведение более глубокой правовой проверки не требуется, поскольку права на программное обеспечение подтверждены записью в государственном реестре и свидетельством о регистрации. Между тем такая позиция представляется ошибочной, поскольку необходимо учитывать правовую природу регистрации программы для ЭВМ, осуществляемой Роспатентом. Применительно к программным продуктам такая регистрация не является правоустанавливающей, она не подтверждает возникновение или принадлежность исключительных прав на ПО, а лишь фиксирует представленные заявителем сведения о заявленном объекте, его правообладателе и авторах. Указанные сведения могут быть впоследствии оспорены или опровергнуты. Поэтому сам по себе факт регистрации ПО не исключает необходимости более глубокой проверки титула.

Также чтобы минимизировать расходы и оптимизировать свои бюджеты, заказчики нередко требуют от юристов ограничить глубину проверки цепочек передачи прав лишь последним или, в лучшем случае, двумя

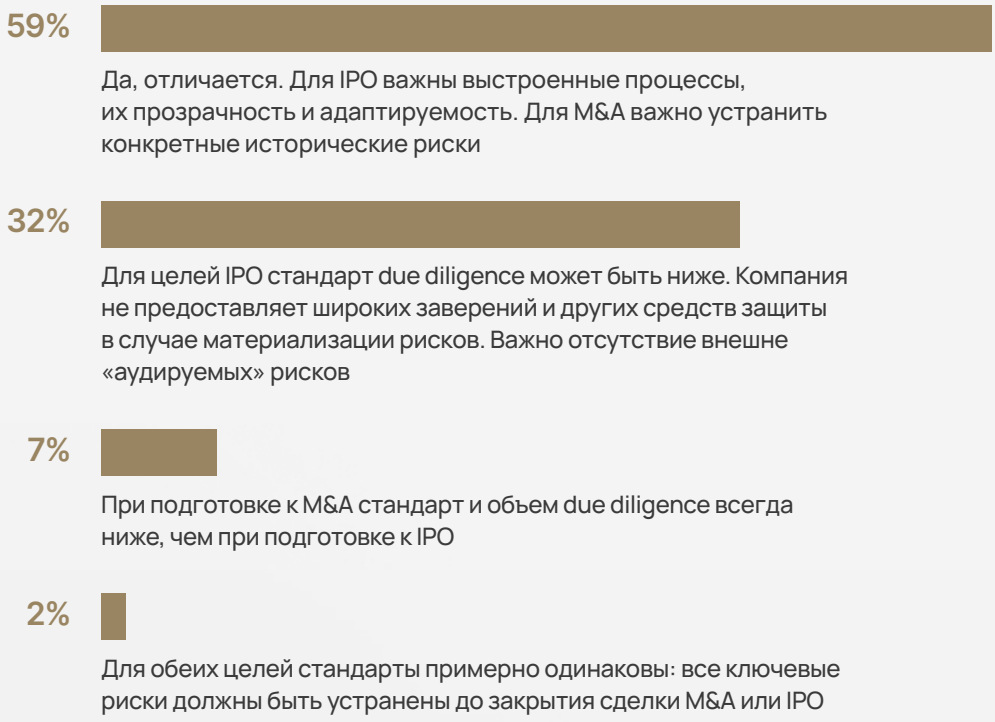
последними звеньями. Существует расхожее мнение, что такого анализа должно быть достаточно для подтверждения перехода прав на ПО к компании-таргету.

Однако важно учитывать, что при таком подходе проверка становится исключительно поверхностной. Она не позволит выявить юридические пороки, возникшие на более ранних этапах создания или передачи актива. Вследствие этого высока вероятность пропустить критический риск отсутствия титула на ПО, являющегося фундаментом ИТ-бизнеса. Следует понимать, что дефект в первоначальном возникновении и передачи прав (например, при оформлении отношений с исходными авторами или иными правообладателями) делает все последующие звенья передачи юридически несостоятельными, что может привести к утрате контроля над ключевым активом.

Объем due diligence для целей M&A и IPO

#РЕЗУЛЬТАТЫ_ОПРОСОВ

Отличается ли объем due diligence IT-компании при ее подготовке к сделке M&A и выходу на IPO?



По данным Опроса по аспектам Tech M&A (41 респондент).



Василиса Лопатина

юрист практики
«Рынки капитала»

VERBA LEGAL

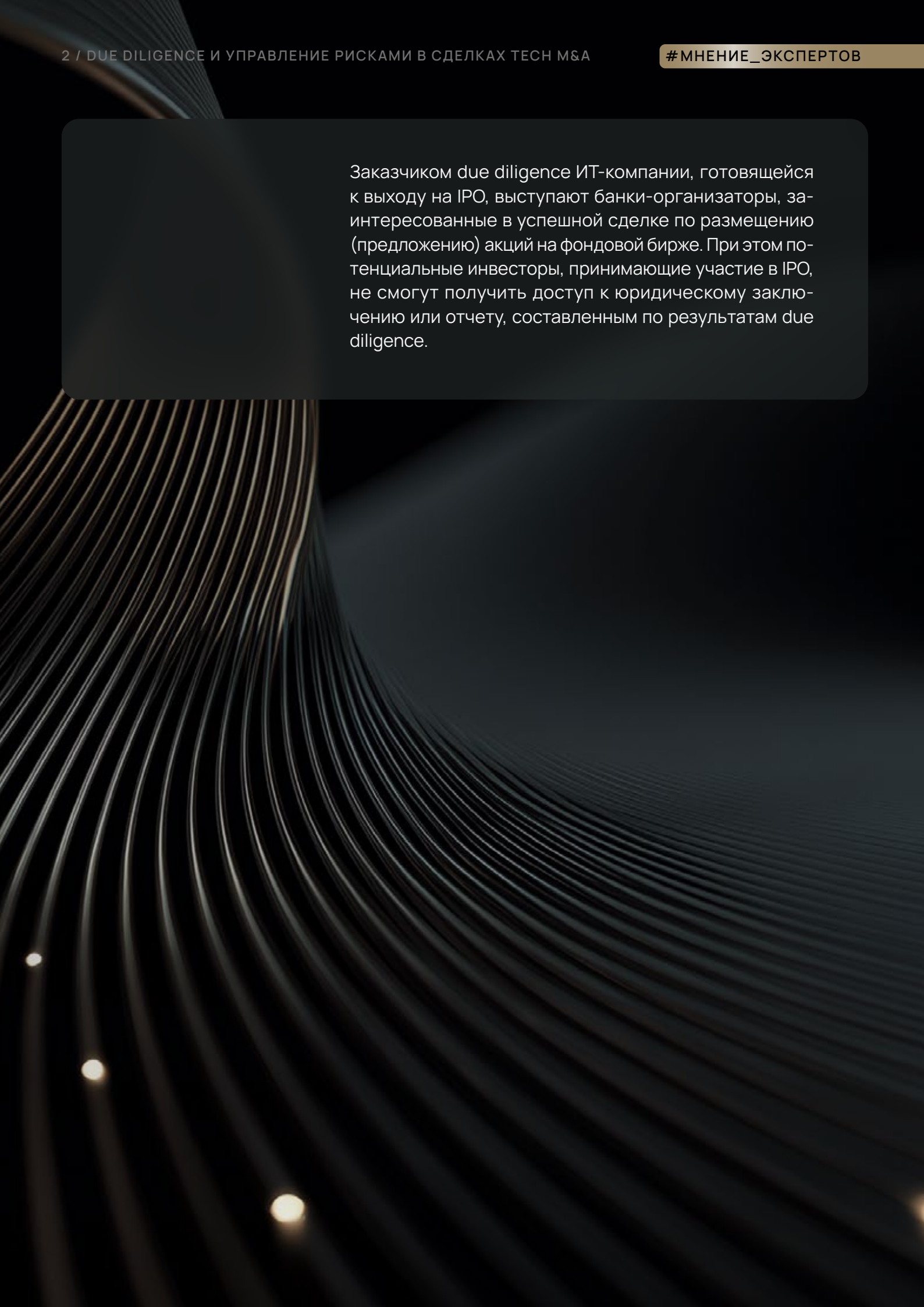
Стандарт и объем юридической проверки ИТ-бизнеса при его подготовке к сделке M&A и к выходу на IPO действительно различаются.

Как правило, на этапе подготовки ИТ-компании к сделке M&A проводится полноценный due diligence, включающий в себя проверку различных аспектов деятельности компании: корпоративного блока (создание компании, титул на доли в уставном капитале (акции) компании, корпоративное управление и так далее), прав на объекты интеллектуальной собственности, движимое и недвижимое имущество, соблюдения трудового и специального законодательства. Цель такой проверки — выявление имеющихся рисков и разработка мер по их минимизации.

В большинстве случаев лицом, заинтересованным в проверке, выступает потенциальный покупатель ИТ-бизнеса. В результате due diligence ИТ-компании покупатель сможет: (i) оценить объект с учетом выявленных рисков и принять решение о покупке доли в компании (share deal) или прав на отдельные активы компании (asset deal), (ii) подготовить список действий (условий), которые необходимо совершить (выполнить) до даты закрытия сделки (например, оформить права на интеллектуальную собственность, вывести из периметра сделки нежелательный актив), а также (iii) сформировать список заверений об обстоятельствах, имеющих место на дату совершения сделки и дату ее закрытия.

При выходе ИТ-компании на IPO, напротив, due diligence имеет ограниченный характер и сводится к анализу правоспособности ИТ-компании и соответствия дополнительного выпуска акций действующему законодательству, а также наличия у ИТ-компании прав на объекты интеллектуальной собственности и иные значимые для бизнеса активы. Например, для провайдеров сервисов ИТ-инфраструктуры, оказывающих услуги колокации, важное значение также имеют права на объекты недвижимости, в которых размещены дата-центры.

Заказчиком due diligence ИТ-компании, готовящейся к выходу на IPO, выступают банки-организаторы, заинтересованные в успешной сделке по размещению (предложению) акций на фондовой бирже. При этом потенциальные инвесторы, принимающие участие в IPO, не смогут получить доступ к юридическому заключению или отчету, составленным по результатам due diligence.



1.2 Ключевые риски, выявляемые в рамках юридического due diligence IT-компаний

При проведении юридических проверок в рамках сделок Tech M&A специалисты регулярно выявляют **ряд рисков системного характера**, которые встречаются в большинстве проектов. Эти уязвимости обусловлены в том числе спецификой IT-индустрии и «молодостью» рынка сделок с технологическими активами, существенную долю которого составляют т. н. венчурные инвестиции, не предполагающие углубленного анализа рисков. Проекты более зрелых стадий, которых в 2025 г. в сегменте Tech M&A было большинство, часто «наследуют» юридические дефекты, оставшиеся неурегулированными в рамках сделок предыдущих раундов. В будущем такие последствия «перелечивать» гораздо сложнее, особенно если ранее их пытались устранить неподходящими для этого методами или решениями. Поэтому чем «старше» актив, тем строже должен быть подход к анализу рисков.

1.2.1 Наиболее распространенные риски

Мы попросили респондентов онлайн-опроса отметить, какие юридические, регуляторные и налоговые риски, выявляемые по итогам due diligence IT-компаний, встречались **им наиболее часто** и какие из них можно назвать **типовыми**.

#РЕЗУЛЬТАТЫ_ОПРОСОВ

Какие риски, выявляемые при due diligence ПО, вам встречались наиболее часто / вы могли бы назвать типовыми / наиболее распространенными?



По данным Опроса по аспектам Tech M&A.

Как показали итоги опроса, участники сделок Tech M&A на практике чаще всего сталкивались с двумя типами рисков: (i) отсутствием титула на ключевое ПО (**88% респондентов**) и (ii) наличием оснований требовать выплаты авторского вознаграждения за созданное ПО (**63% респондентов**). Остальные категории рисков встречались несколько реже (ответы респондентов расположились в диапазоне **32–51%**). Но их тоже можно считать системными, выявленными в трети или половине сделок.

Риски отсутствия титула на ключевое ПО

Риски, связанные с дефектами титула на ПО, очень широко распространены. Основная причина этой проблемы в том, что на ранних стадиях реализации проекта **вопросам документального оформления разработки продукта зачастую не уделяется должного внимания**. Такая ситуация во многом является следствием сложившейся культуры в сфере разработки ПО.

В рамках юридической проверки во многих проектах выявляются существенные недостатки в оформлении документации в отношении разработки ПО. В отдельных случаях — и такие ситуации не редкость — необходимые документы могут и вовсе отсутствовать, поскольку их подготовка откладывалась на более поздний этап. Часто поводом к восстановлению документации служит некое событие ликвидности, например, вход инвестора в капитал или сделка по смене контроля. Тогда компания старается в ускоренном порядке устранить накопившиеся уязвимости, в том числе уже выявленные инвесторов по итогам due diligence. Однако сделать это полноценно на этой стадии уже затруднительно. Часть информации утрачена, восстановить историю миграции прав без документов гораздо сложнее, а «найти» всех причастных к разработке авторов, с которыми не были корректно оформлены отношения, может быть невыполнимой задачей.

В результате эти проблемы выявляются уже покупателем в ходе due diligence и, безусловно, оказывают влияние на весь процесс работы по сделке.

#РАСПРОСТРАНЕННЫЕ_РИСКИ_ПО



Роман Головацкий

партнер

DÉNUO

Среди типичных рисков часто встречаются недостатки оформления прав на программные активы таргета, причем не только в части регулирования трудовых отношений с авторами-разработчиками, но также с фрилансерами и иными подрядчиками. Традиционная проблема связана с использованием аутсорсинговых компаний, когда миграцию прав от автора-фрилансера к таргету-заказчику может быть сложно или проблематично отследить.

У стартапов часто отсутствует какое-либо оформление прав на базу продукта или MVP, которое, как правило, создается в то время, когда о надлежащем оформлении создаваемого актива никто не задумывается.

Также среди типичных проблем, которые мы видим в последнее время, можно выделить фрагментацию прав на ключевой актив среди компаний группы таргета. Это характерно для сложных цифровых платформ, когда часть актива может принадлежать одним правообладателям, а часть — другим. Такая ситуация часто имеет место, когда центр разработки продукта со временем смещается (вместе с разработчиками) из одной компании группы в другую. Причем документальное оформление может быть весьма размытым, и документы, касающиеся создания и принадлежности прав на продукт, могут формироваться одной компанией, а фактически он может создаваться разработчиками, имеющими трудовые отношения с другой компанией группы. В таких случаях задачей юридической команды, осуществляющей проверку таргета, должен быть скрупулезный сбор всех «фрагментов» прав и очерчивание круга всех их носителей.

Риски, связанные с невыплатой работодателями авторского вознаграждения авторам-разработчикам за служебные произведения, также выявляются повсеместно. Однако такие риски чаще не являются критическими, так как сами по себе не порочат титул на нематериальный актив.

Дополнительно можно выделить традиционную проблему отсутствия контроля за использованием опенсорсного программного обеспечения.

#РАСПРОСТРАНЕННЫЕ_РИСКИ_ПО



Татьяна Кассирова

советник корпоративной практики

ELWI

В сделке по приобретению мажоритарной доли в сервисе по сбору аналитики онлайн-продаж, в рамках которой мы выступали консультантом на стороне покупателя, нам пришлось столкнуться с большим кругом вопросов, являющихся достаточно распространенными для данного рода сделок. Бизнес был создан несколькими основателями — физическими лицами, чьим фокусом было развитие изначальной бизнес-идеи, но при этом юридические аспекты деятельности компании как с точки зрения ее создания, так и оформления отношений с работниками, поставщиками и иными контрагентами являлись менее проработанными, что создавало дополнительные риски для деятельности компании и, соответственно, для покупателя при ее приобретении. Эти аспекты необходимо было внимательно анализировать в рамках юридической проверки и впоследствии детально прорабатывать и отражать в юридической документации, оформляющей сделку. Особый фокус сделки был направлен на вопросы интеллектуальной собственности — в первую очередь, на надлежащее оформление прав компании на товарный знак, являющийся существенным элементом, формирующим стоимость бизнеса. Также в качестве предварительного условия для закрытия сделки был детально проработан вопрос оформления прав компании на иные объекты интеллектуальной собственности, составляющие ключевое ядро бизнеса.

> **Проекты более зрелых стадий, которых в 2025 г. в сегменте Tech M&A было большинство, часто «наследуют» юридические дефекты, оставшиеся неурегулированными в рамках предыдущих раундов. Такие последствия «перелечивать» гораздо сложнее, и продавцу по этой причине приходится идти на уступки по условиям и структуре сделки.**

Наиболее критичным последствием отсутствия титула на ПО или его существенной части является **возможный судебный запрет по иску фактического правообладателя на использование такого ПО в будущем**. Это означает, что после вступления судебного решения в силу ПО **необходимо будет удалить со всех носителей, включая составные компоненты, в которых оспоренное ПО может являться лишь частью, и не создавать его новые копии**. Последствия таких рисков зависят от степени критичности ПО, в большинстве случаев они связаны с существенными финансовыми потерями.

Выбытие даже части ключевого актива может привести к длительному простою (неработоспособности) продукта и недоступности сервиса, усилению ИБ-рисков, если, например, удаленный компонент выполнял защитную функцию, потере клиентов, срыву контрактов, предъявлению финансовых претензий.

Если ПО невозможно быстро заменить аналогом, в том числе создать его своими силами, то возникает риск нарушения работы зависимых компонентов продукта. Утрата значимого компонента ПО влечет необходимость срочных капитальных затрат, не учтенных в финансовой модели, на которой основана оценка бизнеса.

> **Самым неблагоприятным последствием отсутствия титула на ключевое ПО является судебный запрет по иску фактического правообладателя на использование такого ПО в будущем. Если соответствующий компонент ПО являлся значимым, это может поставить под угрозу работоспособность всего продукта в целом или отдельных его функций, вызвать экономический простой до момента замены ПО, претензии клиентов и отказ от контрактов.**

Авторское вознаграждение

Вторым по степени выявляемости в рамках due diligence респонденты отметили риск предъявления авторами ПО требований о выплате им авторского вознаграждения за создание и использование соответствующих компонентов. «Популярность» этого риска также вполне ожидаема. Однако ему традиционно уделяется меньше внимания. Этот риск не «обременяет» титул на ПО и не «следует» за ним, его сущность сводится к выплате денежной суммы, поэтому **участники сделок обычно не оценивают его как существенный**.

В ходе due diligence часто выясняется, что вознаграждение за создание ОИС, включая ПО, было **установлено работодателем в ЛНА**, тогда как закон требует, чтобы размер вознаграждения определялся по соглашению с работником. ЛНА, являясь односторонним актом работодателя, не отвечает этому требованию. В целом данное нарушение вряд ли является существенным, особенно если вознаграждение исправно выплачивалось. Однако при таком подходе сохраняется вероятность успешного оспаривания работником размера вознаграждения по мотиву того, что он не был с ним согласован.

Еще одно распространенное нарушение, приводящее к указанному риску, заключается в том, что авторское вознаграждение часто выплачивается работнику в составе заработной платы без выделения конкретной суммы, относящейся к созданию ОИС. Это также может стать аргументом в пользу того, что суд сочтет размер вознаграждения не согласованным.

#РАСПРОСТРАНЕННЫЕ_РИСКИ_ПО



Мария Мойш

патентный поверенный РФ,
старший юрист практики
«Интеллектуальная
собственность»

VERBA LEGAL

В рамках проверки ИТ-бизнеса действительно одной из наиболее частых проблем является выплата авторского вознаграждения работникам в случае создания ими служебных объектов интеллектуальной собственности.

В отношении служебных произведений, в т. ч. программ для ЭВМ, ГК РФ не устанавливает размер авторского вознаграждения и позволяет сторонам урегулировать данный вопрос соглашением. Однако на практике подобные соглашения заключаются довольно редко. Гораздо чаще компании устанавливают размер вознаграждения в локальном нормативном акте. Между тем, если отсутствует документ, в котором работник недвусмысленно выразил свое согласие с установленным размером вознаграждения (например, трудовой, гражданско-правовой договор или хотя бы акт приема-передачи), то суд может посчитать, что стороны не достигли соглашения относительно размера вознаграждения.

Отсутствие соглашения между сторонами приобретает особую проблему, когда речь идет о вознаграждении за создание и использование объектов патентного права. В этом случае для расчета будут применяться ставки, установленные Постановлением Правительства от 16.11.2020 № 1848. В указанном постановлении за основу для расчета берется средняя заработная плата работника, а при передаче права на патент третьему лицу — процент от цены сделки. В связи с этим сумма, подлежащая оплате, может быть существенной.

Также на практике распространена выплата компаниями авторского вознаграждения в составе заработной платы без указания конкретной суммы. Но такой подход тоже влечет риски, т. к. суды считают, что в этом случае соглашение о размере вознаграждения не было достигнуто (Определение ВС от 05.06.2020 № 78-КГ20-1, 2-597/2018).

При этом важно отметить, что невыплата авторского вознаграждения не ведет к утрате прав компанией на

служебные объекты интеллектуальной собственности. Но возникают материальные риски: авторы-работники могут обратиться в суд с требованием о выплате авторского вознаграждения в пределах срока исковой давности.

Указанные риски в большинстве случаев минимизируют обязательством продавца компенсировать имущественные потери покупателя в случае предъявления претензий со стороны работников. Однако нередко покупатель может потребовать устранения рисков до заключения сделки. В этом случае с работником заключается соглашение об авторском вознаграждении и производится его оплата.

Риски, связанные с увольнением ключевых сотрудников

Половина респондентов опроса (**51%**) к типовым рискам также отнесла возможность увольнения ключевой команды компании после закрытия сделки, и связанные с этим последствия.

Важно отметить, что риск ухода команды по существу может быть проанализирован в рамках **HR-направления операционного due diligence**. Однако юристы по косвенным признакам также могут установить наличие оснований для материализации такого риска. Например, если в ходе интервью с менеджментом выяснится, что компания не планирует пересматривать систему оплаты труда и мотивационную программу в отношении ключевых работников, после закрытия сделки ситуация не изменится, в оценку бизнеса соответствующие расходы также не закладывались, — это само по себе является фактором соответствующего риска.

В рамках юридической проверки IT-компании данный риск, в первую очередь, оценивается с точки зрения последствий увольнения команды, связанной с разработкой и поддержкой продукта. В случае его материализации, например, если после сделки уволится ключевой разработчик или вся команда, **компания может утратить контроль над соответствующей частью разработки и потерять конкурентное преимущество**. В ходе юридической проверки, в той мере, в которой это позволяет правовой инструментарий, должны быть оценены **риски создания конкурирующего бизнеса**, в том числе в связи с недостаточной мотивацией команды.



Считают, что в 2025 г. менеджмент IT-компаний стал активнее настаивать на equity-мотивации ключевых работников

#РЕЗУЛЬТАТЫ_ОПРОСОВ

По данным опроса, проведенного в ходе исследования, 26% респондентов отметили, что в 2025 г. менеджмент IT-компаний стал активнее настаивать на внедрении программ долевого участия ключевых работников в бизнесе компании (ESOP).

По данным Опроса по аспектам Tech M&A (125 респондентов).

Выводы юридической проверки по вопросам, связанным с рисками увольнения команды после сделки и отсутствием механизмов их удержания, должны быть соотнесены с итогами иных видов экспертизы, в первую очередь операционной или кадровой, и учтены при структурировании сделки.

Налоговые риски

Топ-5 налоговых рисков, выявляемых по итогам tax due diligence ИТ-компаний в 2025 г.:

- Зарплаты в «конвертах».
- Неучтенная выручка.
- Недобросовестные контрагенты.
- Неправомерное применение налоговых льгот.
- Оспаривание экономической обоснованности расходов.



Андрей Шептий
старший юрист налоговой практики VERBA LEGAL

В рамках опроса респонденты отметили две основные категории распространенных налоговых рисков IT-компаний: (i) возможность утраты налоговых льгот, предусмотренных для IT-компаний (такой риск считает системным **49% респондентов**) и (ii) риск налоговых доначислений в связи с переквалификацией гражданско-правовых отношений в трудовые (считает распространенным **44% респондентов**).

Риск утраты налоговых преференций, предоставляемых IT-компаниям, встречается довольно часто. На его материализацию влияет ряд первопричин — некорректное определение доли профильного (квалифицированного) дохода, нарушение правил признания выручки, вследствие чего фактически превышаются «пороги», предоставляющие право на соответствующие преимущества, наличие иных причин для аннулирования аккредитации.

#НАЛОГОВЫЕ_РИСКИ



Андрей Шептий

старший юрист
налоговой практики

VERBA LEGAL

Использование налоговых преференций для IT-компаний (пониженная ставка по налогу на прибыль и пониженные тарифы страховых взносов) сопряжено с рядом сложностей, которые могут привести к доначислениям налогов и штрафам. Поэтому при проведении TaxDD IT-компаний особое внимание должно уделяться оценке правомерности применения налоговых IT-льгот.

В качестве основных проблемных вопросов, которые могут повлиять на возможность применения налоговых IT-льгот, можно выделить следующие:

1. Сложности толкования при определении квалифицированных доходов.

Получение налоговых льгот возможно только при соблюдении условия о том, что доля квалифицированных доходов от IT-деятельности составляет не менее 70% от всех доходов компании. В налоговом законодательстве предусмотрен исчерпывающий перечень квалифицированных доходов. Однако на практике налогоплательщики сталкиваются с неоднозначным толкованием того, какие именно доходы могут быть отнесены к квалифицированным (например, проблемным является вопрос о возможности льготирования доходов IT-компаний, разрабатывающих банковское ПО или вопрос о переквалификации доходов от доступа к ПО в обычные нельготируемые услуги).

При этом ввиду того, что налоговые льготы для IT-компаний начали действовать с 2021 г., на сегодняшний день не сформировалось достаточного массива судебной практики и разъяснений финансовых / налоговых органов, которые бы могли помочь налогоплательщикам при толковании налогового законодательства.

2. Критерий деловой цели.

Налоговое законодательство прямо не запрещает создавать новую IT-компанию внутри группы. Вместе с тем в налоговом законодательстве действует давно известный принцип наличия деловой цели (ст. 54.1 НК РФ).

Его суть заключается в том, что хозяйственные операции должны иметь деловую (бизнес) цель, а не совершаться исключительно по налоговым мотивам.

В связи с этим при создании отдельной IT-компании для получения налоговых льгот компании необходимо подтвердить наличие деловой цели. В целом (в том числе с учетом позиции Конституционного Суда РФ) соблюдение условий для применения налоговой льготы само по себе не может свидетельствовать об отсутствии деловой цели. Поэтому факт перевода IT-команды в отдельную новую компанию не должен автоматически приводить к претензиям налоговых органов даже в том случае, если единственным заказчиком вновь созданной IT-компании являются компании группы.

Вместе с тем важно отметить, что в данном случае на предмет соблюдения критерия деловой цели будет также оцениваться то, какой персонал был переведен в новую IT-компанию. Если в нее были переведены разработчики, иные IT-специалисты и необходимый управленческий персонал, то критерий деловой цели (например, для применения пониженных страховых взносов) соблюден. Если в IT-компанию в целях экономии на страховых взносах переводится персонал, который не имеет особого отношения к IT-деятельности, то возможны претензии налогового органа.

3. Рыночное ценообразование при оказании IT-услуг.

Если IT-компания оказывает услуги своим аффилированным лицам, их стоимость должна соответствовать рыночному уровню. В ином случае налоговые органы могут предпринять попытку оспорить ценообразование в группе компаний и, например, отказать заказчику в учете нерыночных расходов и вычетов по налогу на прибыль и НДС.

Одним из наиболее распространенных налоговых рисков, связанных с деятельностью IT-компаний, является возможность **доначислений налогов и взносов в связи с переквалификацией отношений по разработке ПО** из гражданско-правовых в трудовые. Этот риск связан с традиционно высокой долей внештатных сотрудников, привлекаемых для целей создания и развития IT-продуктов. В IT-бизнесах нередко используются организационные структуры с участием ИП, лиц, имеющих статус самозанятых, или разработчиков без такого статуса. Многие из них участвуют в разработке и тестировании продукта дистанционно, в том числе из-за рубежа, если сфера деятельности компании допускает такой формат и не относится к «чувствительному» сегменту (ИБ, объекты КИИ и т. п.).

Даже при корректном документировании таких отношений и отсутствии проблем с титулом компания может столкнуться с налоговыми рисками. Контролирующие органы в ходе проверки могут обратить внимание **на фактическое содержание отношений**, а не на их форму. Если взаимодействие с такими разработчиками по существу «похожи» на трудовые с точки зрения условий труда (длительность, устойчивость, подчинение внутренним правилам компании, наличие доступов к ресурсам компании, условия оплаты труда, как у работников) и характера задач (ориентированные на процесс, а не на результат) — такие риски являются высокими.

#НАЛОГОВЫЕ_РИСКИ



Бесханум Мамедова

консультант практики цифрового права и интеллектуальной собственности

o2 consulting

Положение сотрудников, которые работают в РФ, но проживают за пределами РФ, во многом остается в серой зоне. Роструд прямо настаивал на территориальном характере деятельности трудового кодекса и указывал на невозможность заключения с лицами, которые не проживают в РФ, именно трудовых договоров и необходимость заключения договоров ГПХ[9].

Судебная практика не так однозначна, и можно встретить позиции, которые не исключают заключение трудового договора с лицом, которое не проживает в РФ, при этом на практике видно, что суды менее лояльно относятся к таким работникам, однако это создает риски преимущественно для самих работников.

Между тем в случае повсеместного заключения с лицами, не проживающими в РФ, договоров ГПХ появляются иные риски. Так, сохраняется возможность переквалификации договора ГПХ в трудовые договоры, что влечет налоговые риски.

[9] Гражданско-правового характера.

Еще одним значимым налоговым риском является возможность признания факта **искусственного дробления бизнеса компании**. В ряде случаев создание отдельных IT-направлений внутри единой корпоративной группы может быть расценено налоговыми органами в качестве инструмента неоптимальной налоговой оптимизации.

#НАЛОГОВЫЕ_РИСКИ



Андрей Шептий

старший юрист
налоговой практики

VERBA LEGAL

Налоговые органы продолжают уделять пристальное внимание дроблению бизнеса в IT-отрасли. Например, если компания специально выделяет непрофильное IT-направление (т. е. те доходы от IT деятельности, которые не признаются квалифицированными) в отдельное юридическое лицо с целью сохранения пропорции для применения налоговых IT-льгот, налоговый орган будет оценивать деловую цель такой реорганизации. Не исключено, что, если налоговый обнаружит, что предметом дробления была единая IT-деятельность, и это не обусловлено какими-либо экономическими причинами, налоговый орган может признать такое разделение искусственным.

Отмена моратория на проверки

Завершение в 2025 г. действия моратория на проведение проверок в отношении аккредитованных IT-организаций повысило градус настороженности инвесторов в отношении ряда регуляторных и налоговых рисков.

Если в предыдущие годы IT-сектор находился в условиях регуляторных послаблений, направленных на поддержку отрасли, то сейчас фокус смещается в сторону обеспечения соблюдения требований законодательства. В 2026 г. усиление внимания со стороны надзорных органов ожидается, в первую очередь, по таким направлениям, как соблюдение **антимонопольного законодательства** (особенно для IT-компаний с крупной долей рынка), **правомерность применения налоговых льгот**, а также соблюдение **требований по защите ПДн**.

В контексте сделок M&A данный фактор требует анализа операционной деятельности приобретаемой компании на предмет готовности к государственному контролю.



Андрей Шептий

старший юрист
налоговой практики

VERBA LEGAL

Важно отметить, что наличие моратория не препятствовало проведению налогового контроля в отношении IT-компаний. Налоговый орган в любом случае проводил камеральную проверку налоговых деклараций, а также мог назначить выездную налоговую проверку IT-компании по согласованию с вышестоящим налоговым органом (при этом по общему правилу на практике территориальные налоговые органы в большинстве случаев назначают выездную налоговую проверку после одобрения вышестоящего управления).

На практике налоговые органы с начала 2025 г. начали направлять масштабные запросы в адрес IT-компаний для уточнения: (i) правомерности применения налоговых IT-льгот и квалификации доходов в качестве выручки от IT-деятельности; (ii) подхода к ценообразованию и методике определения вознаграждения; (iii) деловой цели выделения IT-компании в рамках группы компаний; (iv) состава сотрудников компании для целей оценки искусственного перевода сотрудников, не связанных с IT, для использования льгот по страховым взносам.



Дарья Носова

партнер и руководитель
практики цифрового
права и интеллектуальной
собственности

o2 consulting

С 31 декабря 2025 г. истек введенный с марта 2022 г. мораторий на плановые неналоговые проверки для российских аккредитованных ИТ-компаний, включая проверки со стороны Федеральной антимонопольной службы (ФАС). Теперь ИТ-компании не обладают иммунитетом на проверки, что может создать дополнительные риски для бизнеса.

В конце 2025 г. ФАС представила новый законопроект, направленный на устранение еще одного иммунитета, касающегося правообладателей интеллектуальной собственности, что применительно к ИТ представляет важную зону внимания.

Нормы ч. 4 ст. 10 и ч. 9 ст. 11 Закона о защите конкуренции сейчас исключают действия правообладателей из-под антимонопольных запретов, позволяя им в определенных случаях избегать ответственности за нарушение антимонопольного законодательства. Этот иммунитет существенно ограничивает возможности ФАС по проведению проверок и привлечению ИТ-компаний к ответственности. При этом давно известна нацеленность регулятора на преодоление (а лучше — отмену) так называемой монополии правообладателей.

Согласно пояснительной записке к законопроекту, ФАС считает, что действующие иммунитеты дают правообладателям, обладающим рыночной властью, возможность злоупотреблять доминирующим положением и ограничивать конкуренцию, например, через завышение цен. Примеры таких злоупотреблений, по мнению ФАС, можно наблюдать на рынках программного обеспечения и контрольно-кассовой техники, где иммунитеты используются как правовое прикрытие для монопольного ценообразования и навязывания невыгодных условий. В связи с этим отмена иммунитетов рассматривается ФАС как необходимая мера для восстановления баланса между защитой исключительных прав и обеспечением конкуренции.

Однако отечественные ИТ-компании выступают против данного законопроекта. Они считают, что он, расширяя полномочия ФАС, устраняет правовые гарантии для правообладателей, при этом перекладывает бремя доказательства конкурентной добросовестности на бизнес. По мнению компаний, это создаст правовую неопределенность, снизит инвестиционную привлекательность и затруднит развитие инновационных технологий в стране.

Таким образом, истечение моратория на плановые проверки и возможная отмена иммунитетов для правообладателей создают дополнительные риски для компаний, работающих в сфере инноваций. В свою очередь, предсделочные проверки должны быть соответственно откалиброваны, чтобы учитывать новые реалии.

Санкционные риски

32% респондентов опроса отметили санкционные риски в качестве наиболее часто встречающихся в сделках Tech M&A. Данная категория рисков имеет существенное значение в тех случаях, когда ключевой актив приобретаемой компании **опирается на зарубежные компоненты ПО** или иным образом **зависит от иностранных лицензий либо сервисов**. В такой ситуации инвестору следует проанализировать цепочки поставок зарубежного ПО или IT-оборудования, наличие у него отечественных аналогов, возможность его использования после закрытия сделки, экспортные ограничения, применимые к его распространению и использованию на соответствующей территории.

#РЕЗУЛЬТАТЫ_ОПРОСОВ



Считают, что в 2025 г. покупатели и приобретаемые активы стали тщательнее проверять взаимные комплаенс-риски (санкционные, регуляторные, KYC)[10]

По данным Опроса по аспектам Tech M&A.

По мнению **20% респондентов**, в связи с ужесточением санкционного давления в 2025 г. участники сделок стали тщательнее проводить KYC-процедуры и усилили внимание к вопросам **взаимного санкционного комплаенса**. Это особенно актуально при наличии в сделке иностранного элемента на стороне продавца.

В 2025 г. санкционный фактор все еще являлся основным драйвером реструктуризаций трансграничных IT-бизнесов. Разделение активов на российскую и зарубежную части нередко являлись вынужденным решением при невозможности оптимизировать структуру сделки с учетом приемлемого уровня санкционных рисков. Также наличие санкционных рисков может повлиять на структуру сделки в сторону ее существенного усложнения.

[10] С полными результатами опроса можно ознакомиться на стр. 57 исследования.

1.2.2 Критичные риски

В ходе исследования мы попросили Tech M&A экспертов отметить, какие риски, связанные с IT-аспектами, они считают **критичными**, способными повлиять на судьбу сделки или требующими существенного пересмотра ее условий.

#РЕЗУЛЬТАТЫ_ОПРОСОВ

Какие риски, выявленные по итогам due diligence ПО, вы считаете наиболее критичными?



По данным Опроса по аспектам Tech M&A (41 респондент).

Как показали результаты опроса, наиболее критичными рисками респонденты считают **отсутствие у компании прав на ключевое ПО** (**93% респондентов**), а также **невозможность оперативной «пересборки» продуктового контура** с целью консолидации компанией прав на весь актив (**61% респондентов**).

Сильная фрагментация прав на ПО нередко связана с наличием в структуре бизнеса зарубежного сегмента, для функционирования которого может создаваться отдельная версия ПО, основанная на общей кодовой базе с российским продуктом. Если компания намерена сохранить иностранный контур бизнеса, «зарубежная версия» продукта может быть выведена продавцом из периметра проверки. Даже если рынки таких продуктов не пересекаются, подобная ситуация может не устроить покупателя, поскольку продавец **фактически сохраняет контроль над тем же продуктом**, что и до сделки, только в иной оболочке.

Как показывает практика, наличие критических рисков, связанных с ПО или иными IT-активами, далеко не всегда приводит к срыву сделки. В большинстве случаев стороны находят компромиссный вариант структурирования сделки с учетом выявленных рисков.

#КРИТИЧНЫЕ_РИСКИ



Александр Венгранович

управляющий директор, начальник управления слияний и поглощений

СОВКОМБАНК

В качестве дилбрейкеров в 2025 г. можно назвать:

- критически неустойчивое качество выручки или непреодолимую концентрацию клиентской базы, churn / retention, уровень скидок и маржинальности, реальность пайплайна;
- неустранимые дефекты цепочки прав на IP;
- риск ухода ключевой команды при отсутствии механизмов удержания.

#КРИТИЧНЫЕ_РИСКИ



Роман Головацкий

партнер

DÉNUO

Критическим вопросом практически всегда является принадлежность титула на программное обеспечение. Основная проблема возникает тогда, когда юристы, осуществляющие проверку, не могут полностью проследить цепочку миграции прав. Такое часто происходит, когда компания-таргет подготавливается под сделку заблаговременно и в ней собираются права на различные компоненты ПО, которые до этого находились на балансе других компаний. Причем если программный продукт имеет длительную историю эволюции, звеньев в цепочке миграции прав может быть много. Тем не менее при проведении проверки важно отследить все переходы титула с момента появления MVP, потому что «обрыв» в части прав в каком-либо из звеньев ставит под вопрос принципиальное наличие у таргета титула на программный продукт или, по крайней мере, его часть.

Следует отметить, что продавцы нередко находятся под влиянием заблуждения о том, что наличие у таргета регистрации ПО в Роспатенте и / или в реестре отечественного ПО автоматически «лечит» все историче-

ские проблемы с правами, поэтому не уделяют должного внимания корректному оформлению их передачи.

Также проблемной может стать ситуация, когда до сделки продавец «расщепляет» права на программный продукт, формируя у себя несколько автономных версий продукта и отчуждая отдельные версии другим компаниям группы. Такой подход нередко встречается, если продавец намеревается продать российский сегмент своего бизнеса и оставить за собой международный. Для покупателя такая ситуация может стать фактором, препятствующим совершению сделки, поскольку без проведения технического аудита выделенной и отчужденной версии продукта и без понимания ее отличия от исходной версии покупатель рискует остаться без прав на продукт или его критическую часть.

#КРИТИЧНЫЕ_РИСКИ



Алексей Дарков

советник, руководитель практики «Интеллектуальная собственность»

VERBA LEGAL

Результаты опроса отражают наиболее критичные болевые точки сделок с ИТ-активами. Неудивительно, что на первом месте респонденты назвали критичным отсутствие титула на ключевое ПО. На практике наличие или отсутствие титула воспринимается сторонами сделки диаметрально противоположно. После введения реестра отечественного ПО, для включения в который удобным стало предъявить свидетельство о депонировании Роспатента, IT-компании первым делом заявляют, что все зарегистрировано. Что ПО есть и в Роспатенте, и в реестре отечественного ПО. Покупатель в таком случае все равно проверяет цепочку возникновения и перехода прав, оценивает, действительно ли объект, который он приобретает, является собственностью продавца. Сама по себе регистрация ПО носит характер оспоримой презумпции, поэтому особых гарантий покупателю не предоставляет, если нет подтвержденной цепочки прав от авторов.

61% респондентов указали на невозможность консолидации прав как фактор, способный сорвать сделку. Здесь мы видим влияние санкционной среды: если в группе компаний — продавце права на ПО рассредоточены между юрлицами в недружественных юрисдикциях, то юридическая «сборка» актива в едином контуре становится либо невозможной, либо сопряженной с чрезмерными налоговыми и правовыми издержками. На практике такие ситуации сейчас не так часты, но любые санкционные риски всегда выступают как дополнительный высокий риск при первичном рассмотрении. Тенденция такова, что инвесторы просто требуют от продавцов предварительной «очистки» структуры владения ПО до выхода на сделку.

Интересен и кадровый блок рисков. Почти половина участников отметили угрозу ухода tech-команды как критичную. Это показывает, что в ИТ-секторе ценность сделки определяется не только кодом, но и людьми, которые способны этот код поддерживать и развивать. Сам код нечасто выступает в качестве самостоятельного предмета сделки.

Отдельно стоит отметить риск локализации компетенций в недружественных странах (41%). Вопрос ухода команды может не стоять, но сейчас, как мы видим, этот фактор может потенциально блокировать сделку. В этом смысле текущая геополитика напрямую формирует M&A-практику.

Несмотря на указанные ответы, на практике чаще встречается подход, когда сделка по приобретению IT-бизнеса проводится даже при наличии тех или иных рисков. Общий тренд: программное обеспечение рассматривается не как статичный актив, а как «живой» бизнес, ценность которого определяется одновременно правами, людьми и бизнес-моделью, которые могут быть скорректированы по итогу проведенного DD.

#КРИТИЧНЫЕ_РИСКИ



Софья Смирнова

советник M&A
и корпоративной практики

O2 консалтинг

Все отмеченные вопросы являются так или иначе существенными и очень значимыми при формировании документации по сделке. С позиции собственного опыта я бы отметила, что риск отсутствия титула на критичное ПО в большинстве стандартных случаев принципиально митигируем подписанием корректных документов и урегулированием отношений с авторами (и лишь иногда, при выявлении особых обстоятельств, может стать дилбрейкером), в то время как невозможность консолидации прав на все ПО в рамках сделки (61% респондентов) и высокий риск увольнения tech-команды в результате смены контроля (49% респондентов), а также нахождение команды или инфраструктуры в недружественных странах (41% респондентов) являются особенно важными при принятии принципиального решения идти в сделку. По нашему мнению, для качественного legal due diligence необходимо включать данные вопросы в периметр юридического анализа и действовать в синергии с коммерческой командой.

Что касается остальных моментов, отмеченных как ключевые в опроснике (неопределенность в хранении экземпляра продукта или особенности договорного оформления бизнес-модели), полагаем, что данные вопросы в ряде случаев должны быть урегулированы продавцом в процессе интеграции бизнеса после сделки или в крайнем случае должны быть определены сторонами перед сделкой при завершении технической проверки.

#КРИТИЧНЫЕ_РИСКИ



Екатерина Третьякова

советник

VERBA LEGAL

Несомненно, риск отсутствия или оспаривания титула на ПО является наиболее критичным и требует первоочередного внимания. Как показывает практика, он достаточно быстро выявляется уже на этапе первичного анализа документов: если в компании не налажены процессы по оформлению служебных произведений и передачи прав, то вероятность проблем очевидна. При этом излечение подобных рисков в целом понятно практикующим юристам, специализирующимся на IT M&A: есть отработанные механизмы подтверждения прав, заключения соглашений с разработчиками и тд.

Однако нельзя сказать, что такой риск встречается абсолютно в каждом проекте — есть команды, где работа с ИС выстроена безупречно. И именно в этих случаях на первый план выходят менее очевидные, но не менее значимые риски. Ключевыми здесь становятся вопросы, напрямую затрагивающие устойчивость бизнес-модели после закрытия сделки: отток ключевых сотрудников либо утрата налоговых ИТ-льгот. В отличие от «титульных» рисков, эти проблемы не имеют универсального решения и зачастую требуют индивидуального структурирования сделки. Именно поэтому при их обсуждении с клиентом масштаб последствий становится особенно очевиден.

Позитивным сигналом можно считать то, что респонденты уделяют внимание вопросам экспортного контроля и совместимости приобретаемого продукта с зарубежным open source. На мой взгляд, это направление заслуживает отдельного анализа: при поверхностном подходе именно «невидимые» элементы кодовой базы (библиотеки, лицензии, авторы из «санкционных» юрисдикций) могут стать источником серьезных правовых и экономических ограничений. В таких ситуациях тесное взаимодействие юридической и технической команд due diligence позволяет выявить риски на ранней стадии и выработать реалистичные меры их нивелирования.

34% респондентов считают критичным риск утраты компанией конкурентных преимуществ, включая создание параллельного бизнеса текущими участниками компании.

Помимо рисков увольнения команды после закрытия сделки, покупателю важно оценить, **были ли такие ситуации в прошлом и каковы их причины**. Если ключевой работник покинул компанию незадолго до сделки, особенно если его вклад в развитие продукта был существенным, не исключен риск **создания конкурирующего бизнеса уже к моменту сделки**. Если компания не сможет документально обосновать принадлежность ей исключительного права на часть оригинального продукта, созданного таким работником, и недобросовестность его действий, существует риск привлечения к ответственности за нарушение авторских прав третьего лица (такого сотрудника или лиц, в чью пользу он мог передать титул на соответствующие ОИС). Если у компании есть основания подозревать существование конкурирующего бизнеса, она может не сообщить об этом покупателю. Поэтому инвестору следует быть более активным и, при наличии сомнений, провести углубленную проверку или форензик-аудит.

> **Критическая масса титульных рисков с ПО связана с проблемой недостаточного документирования процесса создания продукта, начиная с ранних этапов.**

Если документы, оформляющие отношения с уволенными ключевыми разработчиками, не позволяют подтвердить титула компании на созданные разработки, следует проанализировать зависимость текущей версии продукта от спорной части ПО, которая может принадлежать уволившемуся работнику. Это можно сделать только силами технической экспертизы. Если такой анализ подтвердит, что продукт компании является производным от спорного оригинала, этот риск может оказаться критическим для всей сделки.

#КРИТИЧНЫЕ_РИСКИ



Антон Назаренко

старший юрист
практики интеллектуальной
собственности

Melling Voitishkin &Partners

В качестве примера, когда вопросы due diligence ПО играли важную роль для всей сделки в целом, можно привести ситуацию, когда ключевой разработчик, являвшийся также акционером таргета, покинул проект и начал создавать схожее ПО. Для покупателя этот конфликт породил два вопроса, от ответов на которые зависела вся ценность актива: является ли новый продукт переработкой исходного ПО и нарушает ли его создание и использование исключительные права первой компании? Положительный ответ на любой из этих вопросов угрожал не только будущими издержками на судебные разбирательства, но и полной потерей уникальности продукта на рынке, что обесценило бы всю инвестицию.

Специфика сделок формата asset-deal

Риски, связанные с отсутствием титула на ключевые компоненты ПО, могут быть **особенно критичными для сделок формата asset-deal**. Основными факторами, влияющими на выбор такого формата сделки, чаще всего являются высокие риски общего корпоративного периметра или наличие в структуре компании иных активов, не представляющих интереса для покупателя. Такая структура используется существенно реже, чем более простая модель share-deal.

При реализации сделки по модели asset-deal обычно приобретаются права на ключевые ОИС в составе продукта, а также обеспечивается переход технической команды. Смены контроля в отношении компании не происходит, но продавцом (отчуждателем актива) выступает уже не владелец бизнеса, а сама компания. В этом случае от степени юридической «чистоты» титула на отчуждаемые ОИС в составе периметра сделки зависит наличие у компании права распоряжаться продуктом, а значит — способность надлежаще исполнить сделку.

В отдельных случаях формат asset-deal может потребовать переоформления лицензий на компоненты ПО, которыми компания пользовалась по лицензии, либо заключения сублицензионных соглашений. Любой дефект оснований использования компанией соответствующих ОИС, прежде всего ключевого ПО, может означать невозможность получения приобретателем контроля над частью продукта.

#КРИТИЧНЫЕ_РИСКИ



Роман Головацкий

партнер

DÉNUO

Наиболее остро проблема отсутствующего титула проявляется в тех случаях, когда сделка структурируется в форме asset-deal, поскольку в этом случае предметом передачи выступают конкретные нематериальные активы, а не сама компания. Если у таргета отсутствуют права на передаваемый актив, то, несмотря на любые договорные формулировки, он не сможет передать покупателю больше прав, чем имеет сам. Иными словами, при наличии дефекта титула его передача может оказаться невозможной либо будет осуществлена лишь частично.

Ситуация, впрочем, может оказаться некритичной, если дефект титула затрагивает лишь часть компонентов программного продукта, которые не являются ключевыми (например, в силу недостатков оформления отношений с отдельными разработчиками или иными правообладателями). В таком случае даже если таргет не сможет устранить соответствующий дефект и восстановить титул, у покупателя сохраняется возможность локализовать и изолировать «токсичный» компонент. Соответственно, это не повлияет существенно на возможность дальнейшей эксплуатации программного продукта в целом.

Однако ситуация приобретает принципиально иной характер, если дефект титула касается всего программного продукта или его существенной части. Такое может произойти, если, например, таргет не разрабатывал продукт или его ключевые элементы самостоятельно, а получил права на них от третьих лиц в результате последовательной цепочки передач. При такой структуре порок в одном из звеньев правопреемства поставит под сомнение действительность всех последующих переходов прав. В результате конечный покупатель рискует не получить права на продукт вовсе либо получить их в объеме, недостаточном для его полноценной эксплуатации.

#КРИТИЧНЫЕ_РИСКИ



Маргарита Дивина

партнер практики интеллектуальной собственности

Melling Voitishkin &Partners

Мы рекомендуем проводить полную, всеобъемлющую проверку всей цепочки возникновения и перехода прав на ПО, особенно в сделках по приобретению активов (asset-deal) по следующим причинам:

- Свидетельство о регистрации не является правоустанавливающим документом. Регистрация ПО в Роспатенте носит добровольный характер и лишь создает опровержимую презумпцию наличия прав на определенную дату. Такое свидетельство не подтверждает, что права были корректно и в полном объеме получены от всех авторов.
- Без анализа всей цепочки невозможно выявить скрытые дефекты титула, возникающие из-за некорректного оформления прав. Риски, связанные с этим, нельзя полностью устранить с помощью транзакционных документов (например, с помощью механизма заверений об обстоятельствах). Такие инструменты могут лишь митигировать потенциальные финансовые потери, но сам титул на ПО они не способны «очистить».

В сделках с акциями (share-deal) полная проверка также является желательной, но ее глубина на практике нередко варьируется в зависимости от бюджета, выделенного клиентом на due diligence.

1.3 Риски, связанные с обработкой персональных данных

В 2025 г. регулирование в сфере обработки персональных данных было существенно ужесточено. Так, были **увеличены размеры штрафов** за неправомерную обработку ПДн: для юридических лиц — до 300 тыс. руб., а за повторное нарушение — до 500 тыс. руб. Также были **введены специальные составы административных правонарушений**, в том числе за неисполнение обязанности по уведомлению Роскомнадзора о намерении осуществлять обработку ПДн (штраф для юридических лиц — до 300 тыс. руб.), а также за утечки ПДн. Размер штрафов за утечки зависит от масштаба инцидента, категории ПДн и наличия повторного нарушения. Например, за утечку специальных категорий данных или данных более 100 тыс. субъектов штрафы могут достигать 15 млн руб., а за утечку биометрических ПДн — 20 млн руб., в случае повторных утечек применяются оборотные штрафы.

Вместе с этим **были ужесточены требования к локализации** ПДн при их сборе, в том числе посредством сети Интернет. Также были установлены **требования к обезличиванию** ПДн и методам такого обезличивания. По требованию Минцифры России операторы обязаны передавать обезличенные ПДн в государственную информационную систему Минцифры России для формирования государственных наборов данных. При этом предоставление результатов обработки таких данных иностранным лицам запрещено.

#РЕЗУЛЬТАТЫ_ОПРОСОВ



Считают, что в 2025 г. инвесторы стали больше внимания уделять рискам, связанным с утечками данных и ИБ

По данным Опроса по структурированию сделок Tech M&A в 2025 г. (125 респондентов).

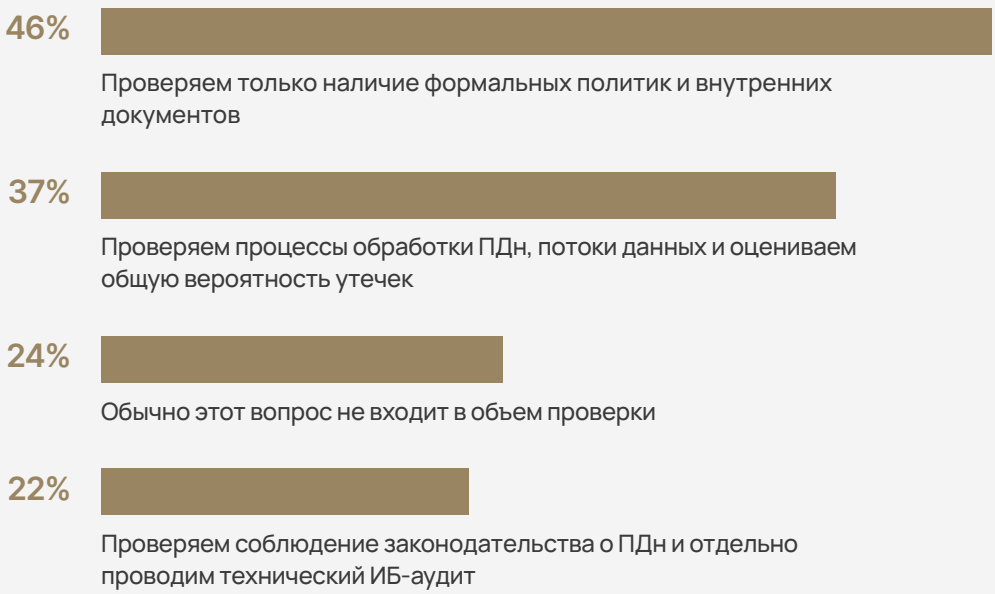
В целом, в связи с ужесточением регулирования сферы ПДн, а также **запуском работы автоматизированной системы мониторинга персональных данных Роскомнадзора** в 2026 г. ожидается увеличение числа проверок. Это особенно актуально, учитывая **изменившиеся критерии отнесения бизнеса к категориям риска**, на которые опирается Роскомнадзор при планировании и проведении контрольно-надзорных мероприятий. Так, например, использование иностранных информационных систем и ПО при сборе ПДн относится по предполагаемой тяжести возможного вреда к самой высокой категории риска (группа «А»). Соответственно, в отношении таких компаний вероятность проверок будет выше.

Таким образом, вопрос организации обработки ПДн выходит из зоны верхнеуровневой документарной проверки и становится значимым направлением due diligence в рамках сделок Tech M&A.

В ходе исследования мы провели отдельный опрос, посвященный анализу рисков, связанных с обработкой ПДн.

#РЕЗУЛЬТАТЫ_ОПРОСОВ

Включаете ли вы в объем юридического due diligence при приобретении IT-компании вопросы защиты персональных данных?



По данным Опроса по аспектам Tech M&A (41 респондент).

Как показали итоги опроса, почти половина респондентов (**46%**) по-прежнему проверяет вопросы обработки ПДн преимущественно по формальным признакам. При этом не уделяется достаточного внимания содержательной оценке процессов их обработки, хранения, уничтожения, передачи и защиты. Однако в новых регуляторных условиях такой подход уже не является оптимальным. Увеличивающиеся риски в сфере обработки ПДн требуют не только формального наличия документов, но и фактического подтверждения организации процессов обработки данных с соблюдением порядка локализации, трансграничной передачи данных, получения согласий, мер по предотвращению утечек и т. п.

> **Использование иностранных информационных систем и ПО при сборе персональных данных относится по критерию предполагаемой тяжести возможного вреда к самой высокой категории риска.**

Если компания оперирует в сегменте B2C — проверка обработки ПДн становится особенно значимой. В этом случае проверки внутренней документации будет недостаточно. Потребуется более тщательный анализ всех процессов обработки ПДн и соблюдения всех применимых требований законодательства.

#ПЕРСОНАЛЬНЫЕ_ДАННЫЕ



Роман Головацкий

партнер

DÉNUO

Вопросы соблюдения требований законодательства о персональных данных в обязательном порядке включаются в объем юридической проверки. Это особенно важно при приобретении бизнеса, для которого обработка значительных массивов персональных данных является ключевым элементом операционной деятельности. В таких случаях оценка системы защиты персональных данных и связанных с ней правовых рисков должна проводиться в расширенном объеме с приоритизацией критичных областей, включая правовые основания обработки, выполнение обязанностей оператора персональных данных, имеющуюся у таргета договорную документацию, локализацию баз данных, трансграничные передачи и т. п.

#ПЕРСОНАЛЬНЫЕ_ДАННЫЕ



Анастасия Мырсина

старший юрист, направление «Защита данных»

/ VERBA LEGAL

В анализируемом периоде юридические департаменты компаний уделяют все больше внимания вопросам защиты персональных данных. Это связано с тем, что законодатель последовательно усиливает меры ответственности и сокращает количество «серых» зон в регулировании. Важным этапом стало вступление в силу в конце мая 2025 г. закона, вводящего оборотные штрафы за утечки персональных данных. Это беспрецедентная мера: ранее подобные санкции применялись в российском праве только в сфере антимонопольного регулирования.

Для соблюдения новых требований недостаточно только грамотной юридической обвязки — корректных форм согласий, актуальных внутренних политик и регулярного обучения сотрудников. Необходима также техническая составляющая. Юридические подразделения, заинтересованные в реальной защите данных, выстраивают тесное взаимодействие с IT-службами и подразделениями информационной безопасности, создавая устойчивый контур защиты.

Подходы компаний к организации этой работы различаются. В одних компаниях проект по обеспечению соответствия возглавляет юрист, в других — представитель IT-функции. Зачастую для оптимизации ресурсов к проекту привлекаются консультанты. Однако наилучших результатов удается достичь, когда эти функции работают в тесном сотрудничестве, совместно обучая, информируя и проверяя бизнес-процессы на предмет соблюдения законодательства о персональных данных.

При этом 2025–2026 гг. стали для компаний не только периодом ожидания правоприменительной практики, но и периодом адаптации к новому уровню регуляторного риска. Устойчивая практика применения оборотных штрафов за утечки персональных данных пока еще не сформировалась, однако сам факт появления таких санкций уже изменил поведение бизнеса: компании активнее оценивают защищенность информационных систем, пересматривают процессы реагирования на инциденты, проверяют договоры с подрядчиками и выстраивают взаимодействие между юридической функцией, IT и информационной безопасностью. В этом смысле законодатель уже во многом достиг превентивного эффекта: персональные данные перестали восприниматься как формальный документооборот и стали рассматриваться как элемент общей устойчивости бизнеса.

Отдельное значение приобрело обезличивание персональных данных. Новые требования и методы обезличивания, применяемые с 1 сентября 2025 г., усилили интерес компаний к тому, как использовать данные для аналитики, исследований, отчетности, развития цифровых продуктов и ИИ-решений без избыточного риска для субъектов персональных данных. На практике это требует не только выбора корректного метода обезличивания, но и описания процесса в документах, оценки риска обратной идентификации, разграничения доступа к исходным и обезличенным массивам и контроля дальнейшего использования таких данных.

#ПЕРСОНАЛЬНЫЕ_ДАННЫЕ



Бесханум Мамедова

консультант практики цифрового права и интеллектуальной собственности

o2 consulting

Большое количество IT-компаний активно используют иностранное ПО в ходе разработки для хранения исходного кода, контроля версий, постановки задач разработчикам, а также включают в свои продукты компоненты, распространяемые на условиях open source лицензий. Также IT компании активно обращаются к иностранным сервисам для сбора, систематизации и хранения данных, в т. ч. персональных данных пользователей, например, применяют иностранные облачные решения, CRM и т. д.

В первую очередь, это риск нарушения требования локализации собираемых персональных данных, в соответствии с которым вся первичная обработка персональных данных должна осуществляться на территории РФ.

Однако ввиду того, что сервера иностранных ресурсов преимущественно расположены не в РФ, то их использование сопряжено с рисками нарушения соответствующих требований.

Таким образом, необходимо провести аудит используемых ресурсов, которые использует компания, на предмет осуществления посредством их обработки ПДн и соблюдения требований локализации, поскольку в определенных случаях даже использование стандартного таск-трекера (например, jira) может повлечь привлечение к ответственности.

Использование таких ресурсов возможно при соблюдении требований законодателя, например, посредством детального разделения процессов обработки, уведомления РКН о трансграничной передаче и администрирования получения соответствующих согласий.

На практике данный вариант крайне сложен в реализации, что в условиях действующего размера ответственности и строгого подхода регулятора делает его менее привлекательным относительно возможных рисков в сравнении с переходом на российские аналоги.

#ПЕРСОНАЛЬНЫЕ_ДАННЫЕ



Илья Булгаков

советник

dénuo

Исторически вопросы персональных данных часто не включались в предмет проверки, однако с ужесточением ответственности в 2025 г. мы все чаще и чаще видим включение данных вопросов в предмет проведения юридических проверок. Причем наличие формальных политик и документов в таргете на самом деле практически ничего не дает в плане понимания рисков утечки, потому что вопросы утечек (за которые сейчас предусмотрены оборотные штрафы при повторном нарушении) — это вопросы дефекта бизнес-процессов (либо их технической составляющей, либо организационной). Мы видим, что примерно с начала осени 2025 г. все больше и больше компаний-покупателей проводят более тщательные проверки соблюдения законодательства о персональных данных (хотя бы общее изучение бизнес-процессов, оценку потоков данных, выборочные интервью с членами команды). Конечно, наиболее часты такие тщательные проверки при приобретении компаний в потребительском секторе. Это связано не только с оборотными штрафами за утечки, но еще и с тем, что формально Роскомнадзор обладает правом на приостановление обработки персональных данных, что может привести потенциально к остановке бизнеса.

#ПЕРСОНАЛЬНЫЕ_ДАННЫЕ



Кирилл Колесников

ведущий юрисконсульт практики интеллектуальной собственности

ЭБР
Юридическая Компания

Персональные данные стали одной из наиболее обсуждаемых тем 2025 г. Введение новых и увеличение старых штрафов, проверки и уголовная ответственность повысили внимание к этому вопросу со стороны юристов и инвесторов. В связи с этим менее четверти респондентов выбрали вариант, при котором проверка соблюдения законодательства о персональных данных не входит в периметр due diligence.

При этом 22% респондентов, напротив, выбрали проведение полноценной проверки соблюдения законодательства о персональных данных, а также ИБ-аудита. У такого подхода есть очевидные преимущества, но есть и два ключевых недостатка — время и деньги. Полноценный аудит займет, как минимум, один месяц, а стоимость проверки может увеличиться более чем на 1 млн руб. Подобное увеличение затрат на due diligence встречается редко, особенно если речь идет о приобретении IT-стартапа.

Наиболее популярными среди респондентов стали промежуточные варианты: проверка наличия формальных документов, которую выбрали 46% респондентов, а также проверка процессов обработки персональных данных и оценка вероятности утечек, которую выбрали 37% респондентов. Однако такие варианты не позволяют полностью закрыть риски нарушения законодательства о персональных данных и одновременно увеличивают затраты на due diligence.

На наш взгляд, в этом вопросе нельзя применять единый подход ко всем IT-компаниям. Если продукты компании не основаны на обработке персональных данных, то при нехватке времени или бюджета проверку в этой части можно отложить. Вместе с тем если продукты компании построены на обработке персональных данных, например SaaS-приложения в сфере медицины, LMS-платформы для школьников и иные подобные сервисы, проверка соблюдения законодательства о персональных данных должна стать полноценной частью due diligence.

Раздел 2

Подходы к митигации юридических IT-рисков

АВТОРЫ



Анастасия Нерчинская



Александр Панов
VERBA LEGAL



Роман Головацкий
DENUO

Краткие выводы

- Подходы к управлению юридическими рисками, выявленными при приобретении технологических компаний, существенно не изменились в 2025 г. по сравнению с предыдущими периодами. Как и ранее, покупатели стремятся максимально снизить уровень рисков до сделки, а продавцы — быстрее заключить сделку, а риски перераспределить с помощью договорных механизмов.

- В 2025 г. сформировался тренд к стремлению покупателей: (i) тщательнее анализировать юридические и регуляторные риски; (ii) максимально устранить критичные риски, выявленные по итогам due diligence, до подписания транзакционной документации.

- Процесс управления рисками, как и ранее, предполагает проведение следующих мероприятий: (i) согласование позиций сторон относительно приемлемости рисков, определения наиболее критичных из них, приоритизации работы по их устранению; (ii) согласование перечня мероприятий фактического характера, направленных на устранение рисков, и их реализация; (iii) предпродажная реструктуризация активов и формирование периметра сделки; (iv) разработка системы транзакционных механизмов защиты покупателя и ее согласование с продавцом и компанией; (v) корректировка положений документов по сделке с учетом устранения рисков до закрытия сделки.

- Большинство юридических M&A-консультантов придерживаются позиции, что если продавец бизнеса не готов обеспечить реализацию мероприятий по митигации рисков до подписания сделки, — это можно сделать в период между подписанием и закрытием сделки. В этом случае в транзакционной документации следует максимально детализировать перечень соответствующих мероприятий.

- По мнению многих участников сделок Tech M&A, существенную часть юридических рисков, связанных с IT-активами, можно устранить путем реализации фактических мероприятий. К ним чаще всего относят корректировку документов, оформляющих отношения по разработке ПО, используемого в составе продукта. Однако такая позиция является, скорее, заблуждением. Далеко не всегда IT-риски, например в отношении титула на ПО, могут быть устранены ретроспективно.

- Если по итогам юридической проверки сделан вывод о невозможности подтвердить наличие у компании исключительных прав на часть ПО в составе продукта, такие риски не могут быть устранены: (i) подписанием документов в рамках трудовых отношений с ретроспективной оговоркой; (ii) заключением соглашений о передаче исключительного права на ПО с ретроспективной оговоркой; (iii) подписанием актов приема-передачи между авторами-разработчиками и компанией, а также любых других документов, «назначающих» каких-либо лиц авторами ретроспективно или «согласующих» наличие у компании исключительных прав на ПО в прошлом, даже если авторы-разработчики согласны подписать такие документы.

- Единственный эффективный инструмент нейтрализации рисков, вызванных отсутствием титула на ПО, — выстраивание цепочки правообладания «на будущее» путем заключения компанией с разработчиками договоров об отчуждении исключительных прав. Устранить ответственность за использование ПО без правового основания в прошлом можно путем заключения лицензионного договора с ретроспективной оговоркой, распространяющей действие лицензии на периоды фактического использования ПО до даты ее подписания. Однако такая лицензия сама по себе не устранит проблему исторического отсутствия у компании титула.

- Заключение договоров об отчуждении исключительных прав между авторами и приобретаемой компанией в целях консолидации прав на продукт может быть сопряжено с существенными налоговыми последствиями. В связи с этим предварительно целесообразно оценить налоговые аспекты всех операций в рамках такой реструктуризации применительно ко всем участникам сделки M&A, включая компанию.

Данный раздел исследования посвящен актуальным моделям управления юридическими рисками в сделках Tech M&A. В целом эти подходы соответствуют стандарту «рыночной практики» и **актуальны для сделок, совершаемых как в 2025 г., так и в другие периоды**.

В 2025 г. из-за **усиления внимания инвесторов к анализу рисков** IT-бизнесов, особенно связанных с титулом на ПО и данные[11], ожидаемо возросли и требования к эффективности работы по их устранению. Заключение сделки с допустимым уровнем риска в 2025 г. стало для многих покупателей не просто более актуальной, но и более сложной задачей. В условиях сложившейся на рынке сделок M&A ситуации «разногласий по оценке» и снижения риск-аппетита инвесторов они чаще стремились **максимально устранить риски до подписания сделки**. Однако сделать это не всегда позволили сроки сделки или переговорные позиции сторон.

[11] См. результаты опросов на стр. 142 главы 1 раздела 3 исследования.

2.1 Общий подход к управлению рисками в сделках Tech M&A

По мнению большинства экспертов, опрошенных нами в ходе исследования, модель управления юридическими рисками при приобретении IT-компаний обычно включает несколько этапов:

- **Проведение переговоров по результатам due diligence**, в ходе которых покупатель оценивает уровень и приемлемость рисков и принимает принципиальное решение о входе в сделку или об отказе от нее, соответственно.
- **Формирование перечня мероприятий** фактического характера, направленных на устранение или снижение уровня рисков. Реализация таких мероприятий обычно начинается до подписания транзакционной документации.
- **Прямая корректировка покупной цены** до подписания документов по сделке. Такие ситуации встречаются относительно редко. Обычно это случаи, когда риск имеет высокий уровень или носит неустранимый характер, но при этом покупатель, при сохранении сделки, не готов перенести его на продавца с помощью договорных инструментов.
- **Разработка комплекса договорных механизмов**, позволяющих перенести часть рисков на продавца в случае их материализации в будущем.
- **Оптимизация структуры сделки** с учетом выявленных рисков. Например, при необходимости продолжения участия основателя в капитале компании для целей мотивации команды на устранение рисков его выход из капитала может быть структурирован поэтапно.
- **Синхронизация с процессом предпродажной реструктуризации**. Часто сделки Tech M&A сопровождаются более широким комплексом мероприятий реструктуризации[12], направленных на создание единого прозрачного и управляемого периметра сделки. Этот процесс, помимо «пересборки» контура ключевых активов, предполагает выстраивание целевой корпоративной структуры, оптимальной для входа приобретателя, с учетом иных интересов (в первую очередь, налоговых последствий) сторон сделки. Процесс реструктуризации может начинаться раньше мероприятий по устранению рисков и идти параллельно с ними.

Мы попросили юристов, сопровождающих сделки с технологическими активами, рассказать, какие подходы к митигации юридических рисков они считают оптимальными, и отметить особенности, характерные для 2025 г.

[12] Более подробно о реструктуризации в сделках Tech M&A см. стр. 69–81 исследования.

#ПОДХОДЫ_К_МИТИГАЦИИ_РИСКОВ



Булат Жамбалнимбуев

партнер и руководитель корпоративной практики

NEXTONS



Ксения Михайлова

советник корпоративной практики

NEXTONS

С нашей точки зрения, наиболее эффективной стратегией является комплексная, многоуровневая система защиты, где каждый механизм дополняет другие.

1. **Действия до закрытия**. Меры, предпринимаемые до реализации сделки, включают в себя фактические действия компании по устранению дефектов. Это помогает минимизировать постсделочные споры и гарантировать покупателю, что действия выполнены не формально, а по существу. Например, заключены договоры, подписаны акты, внесены изменения в свидетельства о регистрации, а также приняты (изменены) локальные нормативные акты и должностные инструкции для предупреждения новых рисков и т. д.
2. **Заверения об обстоятельствах**. Заверения продавца об обстоятельствах помогают покупателю мотивировать продавца и компанию более внимательно и добросовестно проверить текущий статус ПО и датасетов и раскрыть дополнительную информацию, если по какой-либо причине такая информация не была предоставлена во время проведения legal & technical due diligence или появились новые риски после завершения проверок.
3. **Возмещение имущественных потерь**. Этот инструмент незаменим для распределения рисков, которые выявлены, но вероятность и момент материализации которых неизвестны. Например, не всегда наличие не устраненного до сделки дефекта в оформлении прав компании на ПО приводит к тому, что авторы-разработчики предъявят требования о возмещении убытков (выплате компенсации). В то же время покупателю нерационально отказываться от каких-либо договорных мер защиты в этом случае. В таком сценарии обязательство продавца возместить имущественные потери покупателя, если риск реализуется, обеспечивает справедливый баланс интересов сторон.

#ПОДХОДЫ_К_МИТИГАЦИИ_РИСКОВ



Наталья Кузнецова

партнер, руководитель практики M&A и корпоративного права

O_2 консалтинг

Если упрощать, вопрос митигации IP-рисков сводится к выбору между тремя подходами — и здесь наша позиция достаточно прагматична.

Подход 1 (детально прописывать CP[13] с указанием конкретных действий и лиц) — в большинстве случаев мы считаем неудачным решением.

Такая детализация фактически фиксирует в транзакционной документации отсутствие прав на IP на дату signing и создает готовую доказательственную базу. В случае конфликта с разработчиками это может быть использовано против компании и инвестора. Иными словами, вы сами документируете проблему в наиболее чувствительной форме.

Подход 2 (перенос на post-closing без детализации) — допустим, но преимущественно в венчурных сделках и при наличии у инвестора инструментов контроля.

В классических VC-инвестициях (cash-in, фаундер остается в бизнесе) это рабочая модель:

- обязательство формулируется как результат (оформить права), а не как перечень действий;
- детали не раскрываются в КД / инвестиционном соглашении / договоре конвертируемого займа;
- контроль обеспечивается через корпоративные механизмы (совет директоров, согласования).

При необходимости конкретика может выноситься в side letters, но не в «тело» транзакционной документации.

Подход 3 (закрывать риски до сделки и не «светить» их в документации) — в M&A мы считаем базовым стандартом для покупателя.

Если приобретается 100% бизнеса, заходить в сделку с неустраненными титульными рисками и рассчитывать

[13] Conditions precedent — отлагательные условия.

на их последующее исправление — экономически и юридически слабая позиция. После выхода продавца мотивация «чинить IP» резко падает, а leverage покупателя — вместе с ней.

При этом мы не рекомендуем «светить» проблему не потому, что ее нужно игнорировать, а потому что ее нельзя описывать таким образом, который ухудшает позицию покупателя.

На практике это означает:

- избегать детального перечисления проблемных авторов, модулей и договоров;
- использовать более общие формулировки обязательств или условий;
- при необходимости — выносить чувствительные элементы за пределы основной документации.

В реальности, особенно для зрелых таргетов, полное устранение всех IP-рисков до сделки часто невозможно. В таких случаях рынок движется в сторону гибридных решений:

- условные конструкции (SPA с conditions precedent, опционы, framework agreements);
- устранение рисков до closing без их детальной фиксации;
- привлечение независимого консультанта (часто того же, кто делал due diligence) для подтверждения статуса IP после проведенных действий.

Ключевой практический вывод здесь следующий: проблему IP нужно устранять, но не нужно «юридически консервировать» ее в документации.

В связи с реализацией комплекса мероприятий по устранению рисков на практике возникает **ряд вопросов, которые могут быть весьма чувствительными для сторон сделки**.

- В какой срок риски должны быть устранены, чтобы это не сказалось на коммерческих ожиданиях сторон сделки и не затормозило работу основного бизнеса приобретаемой компании?
- Сколько времени объективно понадобится на устранение: (i) критичных рисков; (ii) «средних» рисков; (iii) всех прочих рисков; (iv) всех правовых замечаний, сделанных юристами в рамках due diligence?
- Как встроить реализацию мероприятий по митигации рисков вобщий процесс работы по сделке? Следует ли покупателю подписывать транзакционные документы до устранения конкретных рисков, большинства или всех выявленных рисков? Следует ли предусмотреть выполнение таких мероприятий в качестве отлагательного условия закрытия сделки?
- В сценарии с отлагательными условиями — как покупатель может защитить себя на случай их невыполнения компанией или продавцом? Будет ли покупатель иметь эффективный механизм выхода из сделки, не требующий от него серьезного обоснования или просуживания (сразу или впоследствии) обстоятельств, ставших мотивом такого решения?
- Кто должен нести расходы, связанные с реализацией соответствующих мероприятий, если сделка не состоится?

> **Отсутствие у компании титула в отношении ПО, как и других объектов ОИС, невозможно устранить с ретроспективным эффектом. В отношении периода в прошлом можно лишь устранить риск ответственности за неправомерное использование ПО третьих лиц, например, работников. Однако сам факт перехода исключительного права не может быть перенесен в прошлое.**

Сроки подписания документов по сделке при наличии рисков

Как показали результаты исследования, большинство экспертов придерживается мнения, что для обеих сторон сделки в целом оптимальным решением является **реализация мероприятий по устранению рисков до закрытия сделки**. Неготовность продавца реализовать соответствующие мероприятия до подписания сделки обычно мотивируется отсутствием у него комфорта и уверенности в том, что сделка в принципе состоится. В свою очередь, перенос этих мероприятий на более поздний период, например после закрытия сделки, становится намного более чувствительным для покупателя и требует более серьезного обоснования.



Софья Смирнова

советник M&A
и корпоративной практики

O_2 консалтинг

Несмотря на то, что юридически корректнее просить таргет устранить все риски до подписания сделки, в некоторых коммерческих ситуациях стороны соглашаются, что ряд спорных моментов по титулу (например, подписание документации по служебным произведениям с работниками) может быть отложен на период после подписания сделки (со страховочными механизмами выхода для инвестора). Как правило, это свойственно стартапам, но не зрелым продуктам.

В 2025 г. продавцы чаще были готовы выполнить мероприятия по устранению рисков до подписания документации.

Как показали результаты опросов[14], **47% респондентов** считают, что в 2025 г. при приобретении технологических компаний приобретатели стали более требовательными к анализу и управлению рисками в целом применительно к их различным категориям и видам.



По данным Опроса по аспектам Tech M&A (41 респондент).

#РЕЗУЛЬТАТЫ_ОПРОСОВ

По данным опроса, проведенного в ходе исследования, 35% респондентов отметили что в 2025 г. при приобретении технологических компаний покупатели стали чаще требовать устранения рисков до подписания сделки, а не в рамках периода между подписанием и закрытием сделки.

[14] Более детально упомянутые результаты опроса описаны на стр. 57 и 141 исследования.



Антон Джуплин
партнер
АЛРУД

В нашей практике часто встречается ситуация, когда продавец готов к реструктуризации и мерам по митигации рисков только при наличии юридически обязывающего документа в отношении покупателя. Поэтому чаще используются конструкции с включением отлагательных условий.

Однако в 2025 г. встречались и сделки, где риски устраняются до подписания, особенно когда продавец был не уверен в возможности выполнения всех условий в том необходимом объеме, чтобы покупатель не отказался от сделки и чтобы продавец по итогу получил максимальную цену. Например, в одной сделке 2025 г. завершение предпродажной реструктуризации было отлагательным условием, и к результату такой реструктуризации привязывались KPI по earn-out. Продавец не был готов согласовывать конкретные KPI в обязательственном договоре, поскольку реструктуризация находилась только на начальном этапе и сильно зависела от самого покупателя. Поэтому по итогам переговоров стороны согласовали заключение сразу распорядительного договора (без обязательственного) после завершения реструктуризации. В такой сделке покупатель обычно предусматривает перечень заверений, направленных на подтверждение выполнения действий в отношении устранения выявленных рисков.

Риск отсутствия титула на ПО участники рынка сделок Tech M&A отметили в качестве наиболее распространенного (**88% респондентов**) и критичного (**93% респондентов**). В связи с этим мы попросили ведущих M&A-экспертов уточнить позицию о подходах к митигации рисков на примере именно этой проблемы — т. е. отсутствия у компании прав на ключевое ПО.

#ПРАВОВОЙ_РЕЖИМ



Булат Жамбалнимбуев

партнер и руководитель корпоративной практики

NEXTONS



Денис Борисов

советник корпоративной практики

NEXTONS

По нашему опыту, базовым запросом клиента-покупателя является устранение (митигация) титульных рисков на ПО до подписания сделки. И на практике продавцы, как правило, готовы удовлетворять такой запрос, поскольку это в существенной степени минимизирует риски предъявления требований со стороны покупателя и, соответственно, потери стоимости продаваемого актива в будущем.

Вместе с тем отсутствие обязательственных отношений с потенциальным покупателем (особенно в случае продажи привлекательного актива, на который имеется высокий спрос) не всегда устраивает продавца, поскольку процесс устранения подобного рода рисков является время- и трудозатратным, а также влечет возникновение дополнительных затрат, целесообразность которых может быть неочевидна для продавца при сохранении актива в своем бизнес-периметре.

Как следствие, подписание транзакционной документации с обязательством продавца по согласованному устранению выявленных рисков зачастую выступает разумным компромиссом, поддерживающим баланс интересов между сторонами. При этом важно понимать, что такой подход, как правило, усложняет согласование транзакционной документации, поскольку стороны вынуждены дополнительно подстраивать (т. е., как правило, усложнять) инструменты и договорные способы защиты для симметричного распределения соответствующих рисков (например, в части положений о(б): корректировке размера покупной цены в зависимости от результатов устранения соответствующих рисков; распределении расходов и убытков в случае, если закрытие сделки не состоится; удержании части покупной цены через эскроу; согласовании объема заверений, который будет отличаться на дату подписания и дату закрытия и т. п.).



Дмитрий Позин

партнер

STONEBRIDGE LEGAL

Подход к решению вопроса о том, когда подписывать документы по сделке при наличии титульных рисков на ПО, во многом зависит от критичности таких рисков, характера сделки и переговорных позиций сторон. В нашей практике были разные ситуации. Если риски носят фундаментальный / практически неустранимый характер и ставят под сомнение саму цель приобретения бизнеса, как правило, соглашения не подписываются. В то же время если риски признаются более или менее устранимыми (например, возможно надлежащим образом оформить права / подписать соответствующие соглашения с разработчиками, которые не против передать права приобретаемому бизнесу), то допустима модель с переносом устранения титульных рисков на период с подписания до закрытия сделки. В рамках данной модели в соглашения включаются достаточно детализированные описания в части порядка выполнения соответствующих отлагательных условий / могут даже прикладываться отдельные степ-планы в части устранения титульных рисков на ПО, а также обязательства о возмещении потерь. На случай невыполнения данных отлагательных условий по вине продавца в согласованный срок сторонами может также обсуждаться break-up fee, компенсирующий убытки покупателя, согласившегося «подождать» устранения уже выявленных существенных рисков, будучи изначально связанным юридическими обязательствами по сделке.



Сергей Ханаев

партнер

АЛРУД

В нашей практике покупатели ИТ-бизнеса стремятся к максимальной митигации рисков, связанных с правами на ПО и датасеты, до заключения сделки. Это достигается путем установления широкого и детального перечня отлагательных условий, включающих заключение дополнительных соглашений с работниками для оформления передачи прав на служебные произведения, заключение договоров об отчуждении исключительного права с внешними подрядчиками, не являющимися работниками таргета, или дополнительных соглашений об определении принадлежности таргету исключительного права.

Также подписываются согласия на использование результатов интеллектуальной собственности с подтверждением отсутствия требований к целевому использованию и возражений в отношении такого использования. Важным аспектом является завершение уплаты и документальное подтверждение уплаты вознаграждения по всем договорам.

На период после заключения сделки наиболее приоритетными инструментами являются механизмы возмещения имущественных потерь, позволяющие получить компенсацию, несмотря на осведомленность покупателя о возможных рисках. В дополнение к этому структурируются заверения и механизмы уменьшения покупной цены через положения о качестве товара.

В качестве обеспечения ответственности продавца используется (в том числе в отношении рисков ПО) отложенные платежи (hold back, earn-out). Кроме того, структурно покупатель может входить не сразу на 100% и / или оставлять продавца в качестве ключевого менеджмента на период интеграции таргета после сделки, чтобы сохранить мотивацию продавца на урегулирование проблем (в том числе с ПО) после сделки.

В 2025 г. видим более частое использование модели заранее оцененных убытков, что позволяет более четко определить калькуляцию убытков в условиях неопределенности, учитывая, что непосредственно стоимость самой интеллектуальной собственности может быть незначительной.



Константин Саврыга

юрист

NIKOLSKAYA consulting

Вопрос о подписании и закрытии сделки при наличии неурегулированных рисков, связанных с титулом на ПО, зависит от характера выявленных рисков.

Если риски не являются препятствием для заключения сделки и могут быть устранены в краткие сроки, то устранение таких рисков будет перенесено на период между подписанием и закрытием. Сторонами будет согласован план по устранению (remediation plan), выполнение которого будет являться одним из предварительных условий для закрытия.

Если риски не могут быть устранены в краткосрочной перспективе, либо их устранение не может быть достоверно верифицируемо, либо они являются практически неустранимыми, то покупатель должен принять коммерческое решение о входе в сделку. Если покупатель выбрал идти в сделку, то устранение таких рисков переносится на стадию после закрытия.

Так как покупатель уже вошел в бизнес, то документы по сделке должны предусматривать обязательства продавцов по возмещению потерь покупателя в случае реализации титульных рисков в отношении ПО.

При этом наличие таких обязательств не является защитой само по себе, так как покупателю необходимо обеспечить реальную возможность компенсации своих потерь. Добиться этого можно путем сочетания нескольких механизмов:

- если риск реализовался в течение краткого периода после закрытия сделки и лишил ее коммерческой целесообразности, то покупатель должен иметь возможность выйти из сделки. Это поможет обеспечить возврат покупной цены и выход из проблемного актива;
- если риск реализовался за пределами первоначального периода, но в среднесрочной перспективе, то покупатель может обеспечить исполнение продавцами своих обязательств по возмещению потерь

через установление права на односторонний зачет / уменьшение покупной цены, которая должна быть уплачена продавцам по earn-out или опционам (в случае стадиального выхода продавцов);

- если же риск реализовался на длинной дистанции, то покупателю остается только надеяться на расширенный срок предъявления требований по ДКП, так как чем дальше реализация риска от даты закрытия, тем меньше покупатель имеет контроля за платежеспособностью продавцов, а согласование дополнительных механизмов защиты на дистанции 5–10 лет является чрезвычайно сложным.



Анастасия Духина

старший юрист практики корпоративного права / M&A

sll
SL LEGAL

Если ПО является основным или одним продуктом деятельности компании или критически важно для ее нормальной деятельности, устранение рисков, связанных с таким ПО, всегда становится отлагательным условием для закрытия сделки. Если же риски в отношении ПО незначительны, их устранение может быть перенесено на период между подписанием и закрытием или даже после закрытия сделки. При этом в наших сделках нередко предусматривались предварительные условия, связанные не только с IT&IP-вопросами, но также такие стандартные условия, как получение согласия финансирующих банков на сделку или уведомление ключевых контрагентов об изменении структуры собственности.



Владислав Абрамов

директор по правовым вопросам

KAMA FLOW

Мы применяем комплексный подход для минимизации (митигирования) рисков, связанных с титулом на программное обеспечение и дата-сеты. В частности, мы предпринимаем следующие меры:

1. Проведение углубленной юридической экспертизы (due diligence). Мы анализируем всю цепочку прав на программное обеспечение и датасеты, включая правоустанавливающие документы (договоры разработки, лицензионные соглашения, акты приемки, историю приобретения / перехода прав, соблюдение условий лицензий при использовании сторонних компонентов (особенно open source).
2. Правовые гарантии и заверения. Мы включаем в договоры соответствующие заверения и гарантии в отношении наличия у компании исключительных прав на ПО, а также отсутствия споров и претензий третьих лиц. Дополнительно даются заверения о соблюдении условий использования данных и прав на них.
3. В договор закладываются положения об ответственности продавца за нарушение прав третьих лиц, включая положения о возмещении убытков и механизмы компенсации.
4. Для датасетов анализируется происхождение данных, а также соблюдение норм законодательства о персональных данных, если они используются в датасетах.

По мнению экспертного сообщества, **подход к митигации титульных рисков на ПО, которые могут оказать серьезное влияние на сделку, не отличается от сценариев с иными рисками**, в том числе не является более строгим. К титульным рискам на ключевое ПО будут применяться те же принципы митигации, что и к рискам отсутствия прав на товарный знак или наличия задолженности по уплате роялти за использование ОИС перед материнской компанией.

Отлагательные условия

Мы попросили M&A-экспертов из Stonebridge Legal рассказать на примере собственной практики о наиболее распространенных действиях, которые стороны сделок с технологическими компаниями согласовывали в качестве отлагательных условий закрытия сделки в 2025 г.



Дмитрий Кажаев

старший юрист

STONEBRIDGE LEGAL

В качестве наиболее часто встречающихся отлагательных условий для закрытия по сделкам в отношении IT-активов в 2025 г. мы наблюдали, в частности:

1. Доработку IT-актива для его оперативной интеграции в систему покупателя, в том числе путем выделения из него отдельных компонентов, права на которые будут подлежать передаче покупателю на закрытии по сделке.
2. Заключение или продление срока действия тех или иных договоров с продавцом или третьими лицами об использовании или поддержке соответствующего IT-актива, в том числе на период его интеграции в систему покупателя после подписания документации (и / или закрытия) по сделке.

Представляется, что на практике используются в основном следующие подходы к рискам, связанным с титулом на ключевое ПО и / или датасеты: (a) в случае, если рассматриваемое ПО и / или датасет имеют фундаментальное значение для покупателя, последний может настаивать на устранении соответствующих титульных рисков даже до подписания обязывающей документации по планируемой сделке; (b) применительно к менее значимым титульным рискам их устранение может стать отлагательным условием для закрытия по сделке или (c) в отношении еще менее существенных титульных рисков продавец может быть обязан устранить такие риски в режиме исполнения pre-completion obligation, за нарушение которого может быть установлена специальная договорная ответственность, в том числе в фиксированном размере.

Очевидно, что наиболее часто — более чем в половине «технологических» сделок, к работе по которым была привлечена наша фирма, — используемыми подходами к минимизации степени рисков, связанных с титулом на ключевое ПО и / или датасеты, являются подходы, предполагающие возложение на продавца обязанности по устранению титульных рисков в форме установления соответствующего отлагательного условия для

закрытия по сделке или pre-completion obligation продавца.

Более того, документация по сделке в большинстве случаев предусматривает конкретные действия, подлежащие совершению продавцом для выполнения такого отлагательного условия или исполнения принятого им на себя pre-completion obligation, — например, заключение соглашений о передаче прав на ПО и / или датасет с третьими лицами, внесение изменений во внутреннюю документацию с целью четкого разграничения прав на служебные произведения и т. д.

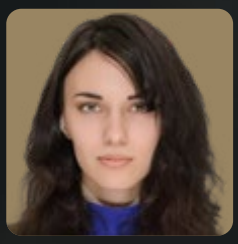
Альтернативный подход

По мнению большинства экспертов, если стороны договорились о реализации мероприятий по митигации рисков в качестве отлагательного условия закрытия сделки, то оптимальным решением будет **максимальная детализация перечня действий и документов**, которые требуется совершить и подписать (соответственно) до закрытия.

Мотивацией такого подхода является обеспечение покупателю большего комфорта при обосновании его отказа от сделки по причине невыполнения продавцом или компанией отлагательных условий. Например, если между конкретным физическим лицом и компанией не будет подписан договор об отчуждении исключительного права на идентифицированное ПО.

Однако в такой ситуации компания в рамках основной документации фактически **прямо подтверждает, что на дату сделки у нее отсутствует исключительное право на спорное ПО**, а также указывает лиц, которым на дату сделки оно принадлежит с большей вероятностью, чем ей самой. При определенных обстоятельствах это может создать в будущем ряд сложностей как для самой компании, так и для сторон сделки.

Преимущества, которые такой подход предоставляет покупателю и, тем более, продавцу, могут быть достигнуты и в случае переноса чувствительной информации на более закрытый уровень коммуникаций. Стороны при разработке перечня мероприятий по снижению рисков обычно тесно взаимодействуют друг с другом, поскольку речь идет о работе с конкретными рисками. Обе стороны понимают, какие действия необходимо сделать, эти вопросы обычно так или иначе остаются на контроле у покупателя.



Анастасия Нерчинская

В случаях, когда хотя бы одна из сторон не согласна с включением излишних деталей, связанных с рисками, в основную документацию по сделке, можно использовать альтернативное решение без принципиального изменения подхода. В частности, стороны могут согласовать документ, предусматривающий все необходимые детали, маркированный особым образом для целей сделки (например, путем парафирования сторонами). При этом формулировка отлагательного условия, используемая в документах по сделке, будет содержать ссылку на такой документ.

Аналогичным образом участники сделок часто описывают мероприятия по реструктуризации, план которой к моменту подписания договора, предусматривающего в качестве отлагательного условия ее завершение, может быть еще не готов. Еще одним примером является подготовка автономного от основного договора письма о раскрытии, когда чувствительные вопросы выносятся за рамки ключевой документации.

> **При принятии покупателем решения о закрытии рисков после подписания документов по сделке важно понимать, что выйти из заключенной сделки по мотиву невыполнения отлагательного условия может быть сложно. Особенно если на стороне продавца выступает физическое лицо, что не редкость в сделках Tech M&A.**

Часто отлагательные условия формулируют посредством комбинации сразу нескольких правовых режимов — как условие и как обязательство или квази-обязательство. В первом случае — это внешнее обстоятельство, обусловливающее действия по закрытию сделки. Во втором — если выполнение условия будет сформулировано как обязанность продавца «обеспечить» его выполнение или «приложить необходимые усилия», — как основание одностороннего отказа от сделки на стороне покупателя по мотиву нарушения продавцом своих обязательств.

Если на подписание каких-либо документов самой компанией продавец отдаленно, но может повлиять, то в отношении ее работников или третьих лиц такая вероятность исчезающе мала. Поэтому если какой-либо документ не будет подписан, продавец, вероятно, сможет обосновать это отказом конкретного работника и доказать, что он предпринял все зависящие от него меры, чтобы выполнить это условие.

Что касается внешнего условия, то если на стороне покупателя будет дискреция принятия решения о его выполнении, не имеет принципиального значения детализация конкретных действий, которые привели к нужному результату, **именно на уровне основного договора**. Если условие будет сформулировано как «наличие у компании исключительного права на конкретное ПО», а в качестве документов, подтверждающих его выполнение, будет указана ссылка на согласованный сторонами перечень, особым образом маркированный для целей конкретного раздела договора, — позиция покупателя вряд ли окажется более уязвимой.

Мнение о необходимости максимально детализировать в основном договоре перечень мероприятий, направленных на устранение рисков, разделяют не все эксперты. В некоторых ситуациях следует оценить, насколько оправдано раскрытие информации, отражающей значимые риски.



Дарья Носова

партнер и руководитель практики цифрового права и интеллектуальной собственности

o2 consulting

Инструмент митигации титульных рисков по IP, который выбирают стороны, по нашей практике, существенно зависит от типа сделки и баланса переговорной силы.

Если речь идет о венчурных инвестициях, большинство которых структурируется через cash-in с сохранением за основателем значительной доли в бизнесе, наиболее оправданным инструментом является включение обязательства по дооформлению прав на IP в качестве обязательства post-closing.

Выступая на стороне фондов и инвесторов, мы, как правило, рекомендуем использовать максимально обтекаемые формулировки — без детального описания того, какие именно договоры должны быть заключены и с какими лицами. При этом ключевым элементом становится механизм контроля: действия компании по оформлению прав должны подлежать предварительному согласованию с инвестором или утверждаться советом директоров с участием его представителя.

Такой подход обусловлен не только гибкостью исполнения, но и управлением юридическими рисками: чрезмерная детализация в транзакционной документации может фактически зафиксировать отсутствие прав на IP на дату сделки и создать доказательственную базу, которая в случае конфликта с разработчиками может быть использована против компании.

При выступлении на стороне основателей общий подход к структуре post-closing обязательств остается схожим, однако в целях повышения определенности для основателя, что примет или не примет как устранение риска инвестор, допустима дополнительная формализация ожидаемых действий — например, через side letters с согласованным планом мероприятий по «сборке» IP.

В противовес этому в классических M&A-сделках, особенно при приобретении 100% долей, перенос устранения титульных рисков на post-closing является для покупателя существенно более рискованной конструк-

цией. После выхода из актива мотивация продавца (и тем более — отдельных разработчиков) к дооформлению прав объективно снижается.

В таких сделках приоритетным сценарием для покупателя остается устранение критичных рисков до signing или, как минимум, до closing. На практике это нередко становится самым длительным этапом подготовки сделки: в одном из наших проектов процесс дооформления прав на ПО занял почти полгода при относительно «молодом» таргете и размере сделки чуть более 1,25 млрд руб.

При этом даже в подобных ситуациях стороны зачастую избегают детальной фиксации выявленных проблем в транзакционной документации. Мы видим распространенную практику использования framework agreement или иных предварительных договоренностей с общим указанием на необходимость устранения IP-рисков, но без их конкретизации.

Для более зрелых и дорогих таргетов полное устранение всех рисков до сделки зачастую экономически или временно неосуществимо. В таких случаях реалистичным компромиссом становятся условные конструкции (SPA с условиями исполнения, опционы, предварительные договоры), однако и здесь мы не рекомендуем детализировать в документации перечень конкретных действий или договоров, подлежащих заключению.

Причины этого носят как юридический, так и практический характер.

Во-первых, сохраняются риски формирования неблагоприятной доказательственной базы в отношениях с разработчиками.

Во-вторых, в процессе «сборки» IP практически неизбежно выявляются дополнительные элементы — новые авторы, модули или иные компоненты, которые не были раскрыты на стадии due diligence. Жестко зафиксированный перечень действий в документации в таком случае ограничивает возможность довести процесс до фактического устранения рисков.

В качестве более сбалансированного решения мы видим привлечение независимого консультанта (как правило, того же, кто проводил due diligence) к процессу устранения рисков с последующей выдачей обновленного заключения о статусе IP. Такая модель не устраняет риски полностью, но позволяет сторонам опираться на профессиональную оценку и снижает зависимость от формальной детализации в договорной документации.

2.2 Эффективность мероприятий по митигации титульных рисков ПО

К основному блоку мероприятий по митигации рисков большинство экспертов относит подписание документов, направленных на устранение юридических дефектов приобретения компанией прав на ПО. Цель этих мероприятий — корректно восстановить цепочку передачи прав на ПО в составе продукта, в отношении которого выявлены титульные риски, от первоначального правообладателя до приобретаемой компании.

При этом важно определить, какие из мероприятий по устранению рисков действительно будут эффективными для всех сторон сделки. А какие — могут лишь усугубить текущую ситуацию и создать «бумажную» видимость устранения рисков.

Мы попросили участников опроса отметить, какие модели митигации рисков они используют в случае, если юридический due diligence выявляет **существенные титульные риски в отношении ПО**. Ответы респондентов приведены на графике ниже.

#РЕЗУЛЬТАТЫ_ОПРОСОВ

Как вы поступите, если due diligence ПО выявит, что на его большую часть права компании не подтверждены?



По данным Опроса по аспектам Tech M&A (41 респондент).

Итоги опроса отражают достаточно зрелый подход к митигации титульных рисков в отношении программного продукта приобретаемой IT-компании.

Абсолютное большинство респондентов (**80%**) отметили понимание того факта, что титульные риски в отношении ключевого ПО в составе продукта могут критично снизить стоимость компании, если его невозможно оперативно или недорого заменить аналогом. Это означает, что «переписать код» за короткий срок не получится. Поэтому под риском фактически окажутся величины прог-

нозных показателей выручки, EBITDA и всех производных от них метрик, а значит, и оценка. Поэтому в этом случае вопрос о прямом уменьшении покупной цены целесообразно адресовать стейкхолдерам покупателя в качестве приоритетного. Однако, как показывает практика, **пересмотр цены до сделки по мотивам высоких титульных рисков с ПО** (в том числе ключевых) **не является распространенным решением**.

С другой стороны, абсолютное меньшинство респондентов (**15%**) считает оптимальным «закрытие» риска отсутствия у компании прав на ПО заверениями, не принимая мер по легитимации титула. Реализация такой опции сама по себе очень рискованна для приобретателя. **Зная о наличии риска, он не может полагаться на такие заверения**. Поэтому в данном случае этот инструмент не будет эффективным.

Более половины участников опроса (**54% респондентов**) считают целесообразным ретроспективное восстановление титула на ПО и цепочки перехода прав. Однако здесь важно понимать, что **ретроспективно наделить приобретаемую компанию титулом в отношении ПО невозможно, если она им ранее не обладала**. Поэтому к вопросу восстановления прав на ПО следует подходить осторожно. Оформление любых документов, «назначающих» компанию правообладателем ПО в прошлом, само по себе не устранит проблему отсутствующего титула.

Значительное число респондентов (**от 34% до 49%**) отметили, что скорее откажутся от ретроспективного восстановления прав на ПО, но при этом будут использовать различные договорные инструменты компенсации в случае материализации титульного риска. Многие респонденты этой категории **считают оптимальным уменьшение покупной цены в случае утраты прав на ПО** на стоимость расходов на его замену ПО или компенсации за простой бизнеса.

Мы попросили представителей юридических M&A-команд и ведущих ИТ-юристов прокомментировать приведенные выше результаты опроса и поделиться своим мнением об оптимальных подходах к митигации титульных рисков.

#МИТИГАЦИЯ_РИСКОВ_ПО



Вадим Перевалов

Восстановление титула на ПО в контексте сделки — сложный и трудоемкий процесс, сопряженный со многими сложностями и дополнительными рисками.

Во-первых, действующее законодательство и судебная практика не позволяют вылечить пороки титула на ПО «в прошлом». Условно, если разработка ПО не входила в обязанности работника и потому ПО не являлось «служебным», нельзя переписать должностную инструкцию и изменить трудовые отношения в прошлом, нельзя оформить передачу прав несколько лет тому назад, нельзя просто «по акту» передать права, которые по закону не могут быть переданы. И уж совсем само собой не стоит в транзакционной документации обязывать другую сторону «найти и предоставить» не существовавшие ранее документы, чтобы покупателю не становиться ответственным за возможный подлог. Передача прав на ПО в таком случае может осуществляться только текущим числом как отдельная сделка.

Во-вторых, если компании не перешли права на ПО от кого-то из разработчиков, это означает, что разработчики и компания являются со-правообладателями, и любые сделки по распоряжению ПО они должны были ранее заключать совместно, а любое использование ПО лицензиатами может быть потенциально признано незаконным. Если не вылечить пороки титула на ПО и ограничиться заверениями вместо восстановления недостающих прав (а именно это происходит в сделках чаще всего), то в плохом сценарии данный риск может привести к полной невозможности использования ПО и разрушению отношений со всеми пользователями-контрагентами. Этот риск менее актуален для внутреннего или облачного ПО, но в полной мере применяется к on-premise и настольному ПО, которое устанавливается заказчиком.

В-третьих, наличие дорогостоящего, но несуществующего ПО на балансе таргета может спровоцировать набор дополнительных налоговых рисков, особенно

когда капитализация осуществлялась в период максимальных ИТ-льгот, а амортизация уже при ненулевом налоге на прибыль (актуально в свете последних налоговых изменений).

Надо понимать, что в реальности риски с титулом на ПО практически невозможно митигировать полностью. Их можно только разумно уменьшить.

Практически всегда существует часть авторов, с которыми компания рассталась на недружественной ноте и которые не согласятся что-либо подписать. Более того, сам запрос о подписании дополнительных документов может навести таких авторов на опасную мысль, как они могут воспользоваться ситуацией. А другая часть авторов уехала из страны. Или вообще окончила свой жизненный путь, и теперь таргету предстоит иметь дело с корыстолюбивыми наследниками.

Восстановить полный список авторов в отношении достаточно давно разрабатывающегося ПО тоже не всегда возможно. Особенно учитывая, что репозитории обычно отражают, кто писал код, но редко отображают, кто проектировал интерфейсы и писал техническое задание либо создавал эссеты, просто сваленные на сетевой диск.

Задача покупателя в таком случае — убедить продавца собрать максимальное число реалистично собираемых документов, особенно учитывая ограниченные сроки сделки. При этом важно максимально переложить на продавца остаточный риск через гарантии и заверения, что означает, что ни переписка, ни транзакционные документы не должны фиксировать избыточные знания покупателя о текущей ситуации и конкретных отсутствующих документах.

#МНЕНИЕ_ЛИДЕРОВ_РЫНКА

Практические проблемы митигации рисков



Роман Головацкий
партнер

dénuo

После завершения юридической проверки неизбежно встает вопрос разрешения выявленных правовых рисков, касающихся программного обеспечения как ключевого актива. Здесь основной фокус должен быть направлен на устранение пробелов в документарном подтверждении титула на программный продукт в целом и его отдельные существенные компоненты.

Наиболее сложной и нетривиальной является работа с историческими рисками. Чем дальше во времени находится выявленный в ходе проверки дефект в правах, тем сложнее его устранить. Это касается ситуаций, когда права мигрировали через длинную многоуровневую цепочку их носителей, и на одном из ранних звеньев этой цепочки имелся порок в должной передаче прав. Компании-предшественники могли сменить владельцев, быть реорганизованы, прекратить существование и быть в целом недоступными для оформления необходимых документов. Также это характерно и для случаев, когда ключевые компоненты создавались людьми, трудовые или гражданско-правовые отношения с которыми давно прекращены, и доступность которых для решения выявленных рисков аналогичным образом проблематична.

Часто встречающимся мифом в бизнес-сообществе является ложная идея о том, что все проблемы с титулом на программный продукт легко устранить путем регистрации его в Роспатенте с указанием «нужных» правообладателя и авторов. Это опасное заблуждение, поскольку государственная регистрация программ для ЭВМ и баз данных в Роспатенте не носит правоустанавливающий характер и не решает проблем с титулом. Напротив, заявление недостоверных сведений при такой регистрации может лишь умножить правовые риски, но не устранить их.

Также в качестве проблематичных способов решения рисков с титулом следует отметить идеи о ретроспективной передаче исключительного права. Например, путем подписания некоего подтверждающего акта, назначающего таргет правообладателем в прошлом при отсутствии на то ранее существовавшей формальной сделки. Такой подход вряд ли можно считать релевантным, ведь отчуждение исключительного права предполагает, что приобретатель получает весь спектр прав, вытекающих из владения титулом (включая возможность распоряжаться исключительным правом и запрещать использование охраняемого объекта), которых, очевидно, при ретроспективной передаче у приобретателя не могло быть, и он не мог их реализовывать. Поэтому нельзя «договориться» о том, что исключительное право перешло, допустим, год назад, это лишь создаст видимость передачи, но не ее факт.

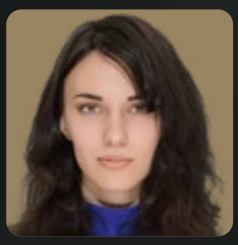
Оформление подтверждающих актов может быть оправданным только в качестве дополнительного инструмента и только в том случае, когда из предшествующей документации однозначно прослеживается факт перехода исключительного права к таргету. Например, они могут быть полезны для документирования реально поставленных перед разработчиками задач через внешний сервис, когда необходимо собрать их в единый общий документ. Однако в случае отсутствия подтверждения передачи титула сам по себе такой подтверждающий акт этот пробел не восполнит.

Аналогичным должен быть подход и для трудовых отношений при подтверждении прав на служебное произведение (ст. 1295 ГК РФ). Если занимаемая разработчиком должность, его обязанности и трудовая функция не подразумевали выполнение работ по разработке программного обеспечения, то оформление подтверждающих актов или новых, детализированных должностных инструкций не поможет устранить дефект титула таргета в отношении ранее созданных объектов.

При таких условиях действенным способом «лечения» риска дефекта титула является заключение договора об отчуждении исключительного права от автора или иного фактического правообладателя таргету. Данный инструмент применим и в контексте трудовых отношений, когда имеющихся доказательств недостаточно для квалификации объекта как служебного произведения. Между тем необходимо учитывать сопутствующие налоговые последствия, возникающие в связи с приобретением нематериального актива.

Если отчуждение исключительного права по каким-либо причинам невозможно, остается вариант локализации и изоляции проблемных частей программного продукта с целью исключения их из его состава. При этом следует учитывать, что в отдельных случаях замена таких частей может быть ресурсоемким процессом, в том числе с точки зрения временных затрат. Однако в противном случае риски, связанные с дефектом титула, перейдут на покупателя.

#МИТИГАЦИЯ_РИСКОВ_ПО



Анастасия Нерчинская

О чем важно помнить при составлении перечня рекомендаций по устранению титульных рисков на ПО (исходим из того, что стороны определили для себя приоритеты в рамках этой задачи, в том числе выделили наиболее критичные компоненты).

1. Не существует никаких «волшебных» приемов, которые позволили бы полностью устранить исторические риски отсутствия у приобретаемой компании титула на ПО. Такие риски очень часто недооцениваются — ряд специалистов считает, что раз в этой сфере не много громких споров с серьезными последствиями, значит, риск низкий, так как его ожидаемая вероятность мала.
2. Получив перечень рисков по итогам due diligence, важно трезво оценить, что реально можно сделать, чтобы устранить или снизить эти риски, **и при этом не создать новых**. Часто в целях «лечения» рисков предлагается провести большую работу, итогом которой фактически может оказаться лишь «создание видимости» устранения рисков. Чтобы этого избежать, важно критически осмыслить весь перечень предлагаемых мероприятий. Это нужно делать с привлечением опытных IP и IT-юристов.
3. Важно сразу исключить **приемы и подходы, которые «не работают»**. Их много, в рамках комментария можно перечислить только основные из них:
   - **Невозможно ретроспективно передать компании исключительное право на ПО** или иной объект ОИС — вне зависимости от того, прошел ли такой объект регистрацию в Роспатенте. П. 2 ст. 425 ГК РФ не применим по отношению к передаче исключительных прав на ОИС, это в том числе подтверждает судебная практика.
   - Дефекты в оформлении документации на ПО, которые стали ключевой причиной вывода об отсутствии у компании исключительного права на него, могут быть очень разнообразными. Но **ни один из них не может быть устранен неким актом приема-передачи** между автором-разработчиком

и компанией (такие документы некоторые специалисты называют confirmatory acts) или любым другим документом, в котором автор и компания договорились бы о том, что права на ПО принадлежат компании, автор подтверждает, что все, что он раньше сделал для компании в связи с разработкой ПО, принадлежит компании, а он не имеет претензий. Акт приемки не является основанием передачи исключительного права. **Если, например, в силу некорректно оформленного режима служебного произведения у компании не возникло исключительное право на ПО в прошлом, то подписание таких «актов приемки» не устранит эту проблему**.

- **В трудовых правоотношениях также не применяется принцип ретроспективного действия**. Нельзя сегодня договориться с работником о подписании дополнительного соглашения к ранее заключенному трудовому договору, в котором будет согласовано, что в его должностные обязанности входит разработка ПО, и при этом придать документу ретроактивную силу, указав, что соглашение вступает в силу с некой даты в прошлом. Изменить ретроспективно ЛНА (например, если должностные обязанности сформулированы в типовой должностной инструкции, утвержденной ЛНА) также нельзя, о чем прямо сказано в трудовом законодательстве.
- Внедрить систему документооборота, регулирующую процесс управления разработкой и развитием ПО, **можно только на будущее время**. Такая система предполагает либо подписание документов (например, дополнительных соглашений к трудовым договорам с работниками, устанавливающих корректное описание должностных обязанностей, вводящих индивидуальные должностные инструкции, порядок передачи компании созданных работником артефактов) и утверждение ЛНА (например, положение о служебных произведениях, об использовании информационных систем в процессе разработки ПО). **Это поможет**

устранить риски только в отношении вновь создаваемых объектов ПО. Во всех остальных случаях сохранятся риски использования ПО без законного основания, например, путем модификации прежних разработок.

4. Следует определить перечень действий, которые **действительно могут быть эффективными** и помогут снизить риски.

   - Во-первых, это обеспечение любого законного основания возникновения / приобретения исключительного права, предусмотренного гражданским законодательством. Самое распространенное из них — это договор об отчуждении исключительного права на ПО. Если в отчете по итогам юридического due diligence указано, что с высокой степенью вероятности (желательно с опорой на данные технической экспертизы) автором и правообладателем конкретного ПО является не сама компания, а третье лицо, и приведено обоснование такого вывода, — **устранить риск можно путем заключения с таким лицом (если оно согласится) договора об отчуждении исключительного права**.

     Также это может быть вклад исключительных прав в уставный капитал (труднореализуемый в массе сценарий, требующий независимой оценки). Если права на спорное ПО находятся у юридического лица, например, одной из компаний группы продавца, возможно проведение реорганизации, что также — исключительно экзотический и крайне редкий сценарий «лечения» рисков на ПО.

   - Во-вторых, это лицензионные договоры или дополнительные соглашения к текущим договорам, которые ретроспективно (в отношении прав использования ОИС ретроспективное действие допустимо) восстанавливают недостающий объем правомочий компании, если в прошлом она вышла за их согласованные лицензиаром пределы или вообще использована ОИС третьего лица без основания.

- В-третьих, это договоры об отчуждении исключительного права на ПО, которые по итогам due diligence оказались за периметром группы, например, у материнской компании, что компанией не оспаривалось и было ей известно. Это — митигация более «простого» риска отсутствия в периметре сделки необходимых IP-активов, где компании изначально известен внешний правообладатель.
- В четвертых, заключение тех самых «уточняющих актов», но только не в отношении передачи титула на ПО. Такие документы носят скорее процессуальный характер, позволяющий компании обосновать, что конкретно было создано, например, ее работником. **Но только при условии, что в отношении него не было выявлено дефектов в оформлении режима служебного произведения**. Однако если режим служебного произведения не был корректно установлен, сам по себе такой акт не поможет, а лишь усложнит ситуацию. Фактически автор ПО — работник, а актом он уточняет, что сделал и передал «в пользу компании» такое-то ПО (далее его описание).

  Подписание таких актов не поможет устранить риск (не передаст компании титул на дату в прошлом) и том случае, если режим служебности будет «вылечен» путем отчуждения исключительного права на будущее время. В этом случае подписание такого акта вообще не будет иметь большого смысла. Идентифицировать ПО можно будет в акте приема-передачи к соответствующему договору об отчуждении исключительных прав.

  Иными словами, такие акты носят вторичный характер, к тому же законом не предусмотрена обязательная форма служебного задания для создания объекта авторского права. Первично — обеспечить наличие титула.
- В-пятых, в случае полной уверенности компании и покупателя в перечне авторов конкретного ПО и изначально правильного оформления всех документов, то есть фактически при отсутствии рис-

ков, можно дополнительно создать презумпцию авторства соответствующих лиц. Например, указать их авторство в исходном коде, документации, а также в некоторых случаях, — добавить «недостающих» авторов в свидетельство о государственной регистрации.

Но, поскольку такие ситуации крайне редки и **в большинстве случаев даже технические эксперты допускают оговорки и сомнения относительно полной точности перечня авторов, такие действия, скорее, не могут быть рекомендованы как общее правило**. Если создать презумпцию авторства одного лица, а по факту автором окажется другое, проблема только усугубится. Более плохой сценарий — когда авторы, которых добавили в свидетельство, откажутся подписать с компанией документы о передаче ей исключительных прав.

#МИТИГАЦИЯ_РИСКОВ_ПО



Наталья Кузнецова

партнер, руководитель практики M&A и корпоративного права

O_2 консалтинг

Не удивительно, что критическое большинство респондентов отдали предпочтение первому варианту (попробовать сразу снизить цену). При этом если бы в продолжение мы задали вопрос о том, в каком количестве сделок это удалось реализовать и снизить цену значительно, то результаты бы существенно отличались.

Действительно, бизнес по сравнению с тем, что было 10 или даже 5 лет назад, готов более серьезно относиться к IP-рискам в технологических проектах. Тем не менее снижение цены или скрупулезное устранение рисков встречаются редко. Обычно мы их видим в сделках покупки 100% бизнеса и крайне редко в инвестиционных сделках или в сделках ранних стадий развития компаний. На моей практике в единичных случаях покупатель озадачивал продавца полным (насколько это возможно) устранением рисков до сделки, несмотря на то, что по оценкам бизнеса «переписать код можно было в целом месяцев за 6.

С другой стороны, в некоторых случаях выявляемые риски по IP невозможно «вылечить», и это иногда становится причиной для того, чтобы в сделку не зайти покупателю (если актив требует существенных последующих инвестиций для развития или нет уверенности в платежеспособности продавца для взыскания с него в будущем убытков в связи с недостоверностью заверений или потерь). В сделках cash-out на стороне покупателя мы стараемся закладывать как механизмы уменьшения цены, так и потерь, включая положения об исключении двойной ответственности. Полагаться исключительно на заверения при текущей правоприменительной практике считаем ненадежным. В сделках cash-in механизмы для защиты инвестора более ограничены, и основным инструментом выступают потери, хотя договоренности о рэтчете и выпуске дополнительных долей инвестором также встречаются, но, скорее, как дополнительный механизм на случай неплатежеспособности основателей и отсутствия у них средств для возмещения потерь инвестору.

#МИТИГАЦИЯ_РИСКОВ_ПО



Илья Булгаков

советник

Dénuo

В нашей практике были случаи полного отказа от сделки вследствие отсутствия прав на ключевое ПО. Однако мы также видели практически все упомянутые ответы, и, как правило, выбор конкретного пути или их комбинации зависит от фигуры покупателя, риск-аппетита и уровня комплаенса. Если покупатель является крупной компанией с сильным комплаенсом (например, публичная компания) или если планируется интеграция ИТ-решения в собственные продукты покупателя, то вопрос прав на ключевое ПО действительно критический. Как правило, вопрос в этом случае окончательно решается на инвест-комитете покупателя, либо вопрос эскалируется на уровень топ-менеджмента. Если покупатель относительно небольшая компания и обладает простой организационной структурой, то может быть комбинация вариантов (обязательство возмещения потерь, положения по удержанию цены и т. д.).

Бывает и так, что покупатель принимает риски, но стратегически принимает решение постепенно разрабатывать приобретенное решение самостоятельно, постепенно заменяя «дефектный» код на свой, или приобретатель может решить постепенно просто «убить» приобретенный продукт, переведя клиентов на себя. В этом случае основным драйвером приобретения компании выступает «покупка времени», когда можно не опасаться конкуренции со стороны конкретного таргета, или «покупка клиентских отношений». В этом случае риски отсутствия прав на ПО менее значимы и существенны с точки зрения намерения покупателя и общего драйвера сделки.

#МИТИГАЦИЯ_РИСКОВ_ПО



Кристина Мкртчян

советник практики
интеллектуальной
собственности
и корпоративного права

ЭБР
Юридическая Компания

Опрос показывает, что рынок не выработал единого подхода, потому что корректного решения не существует (разброс ответов от 80% до 15%).

Лидирующий результат (80% — пересмотр оценки или выход из сделки) понятен, дефект титула на ПО — это не проблема документооборота, а сигнал о том, что компания не является полноценным правообладателем своего ключевого актива. Оценка, которая этого не учитывает, просто неверна.

Дефект, как правило, возникает по одной и той же причине: ПО разрабатывалось годами силами подрядчиков и фрилансеров, договоры с которыми не предусматривали отчуждения права, а трудовые договоры со штатными разработчиками не содержали корректных положений о служебных произведениях. Часть авторов к моменту DD уже недоступна: уволились, уехали, потеряли связь с компанией. Это не исключение, это стандартная история для большинства технологических компаний.

Ретроспективное восстановление документов (54%) — это самый частый первый рефлекс, и именно поэтому важно понимать его пределы. Подписанный сегодня договор об отчуждении права действует с даты подписания, а не с даты написания кода. Риски промежуточного периода он не закрывает. При единичных пробелах инструмент рабочий; при массовом дефекте — нет: процесс растягивается на месяцы, часть авторов недоступна, часть требует компенсацию, а оставшийся незакрытый процент касается ключевых модулей.

Вычет из цены в размере затрат на замену ПО (49%) недооценивает реальный риск: стоимость переписать код — это наименьшая статья. Простой бизнеса, отток клиентов, компенсации правообладателю, — все это в формулу не входит. Indemnity (34%) работает, только если продавец через два года платежеспособен и доступен, что не гарантировано. Заверения (15%) и вовсе создают лишь основание для иска, но не реальную защиту.

Западная практика приходит к тому же выводу, но через более структурированные механизмы. В США действует стандарт 'pre-closing IP cure' как условие закрытия, и если 'cure' невозможен, то применяется специальный indemnity с эскроу около 10% от цены сделки. W&I страхование используется примерно в 60% сделок, но с принципиальным ограничением: дефект, выявленный в DD, страховщик исключит из покрытия.

Итог один: массовый дефект должен быть заложен в оценку, а не «вылечен» документами после подписания.

2.3 Налоговые последствия восстановления прав на ПО

Не существует никаких особых приемов и методов, которые позволили бы полностью устранить исторические риски отсутствия у приобретаемой компании титула на ПО. Если титула нет, например, из-за пороков оформления соответствующих документов, — его можно «восстановить» только на будущее время.

Следует помнить, что мероприятия по восстановлению титульных рисков, связанных с ключевым ПО, могут иметь значительные налоговые последствия. Широко распространена практика, когда при проведении мероприятий по митигации титульных рисков на ПО заключаются договоры об отчуждении исключительного права в пользу компании. Часто в таких договорах, заключаемых между авторами-разработчиками и компанией, размер вознаграждения за отчуждение исключительного права устанавливается в виде символической или иной суммы, которая в любом случае кратно ниже рыночной стоимости соответствующего ПО или его части, и несопоставимо ниже цены сделки.

Известно, что стоимость многих зрелых продуктовых бизнесов может достигать нескольких млрд руб. Ключевой актив такого бизнеса, лежащий в основе его стоимости, — ПО. Поэтому большая часть стоимости компании (в виде будущих денежных потоков[15]) сосредоточена именно в таком активе как ПО и создается именно им. Даже если балансовая стоимость отдельных его компонентов (например, отдельных функциональных модулей) кратно меньше цены сделки.

При этом сделка M&A обычно совершается в относительно непродолжительный срок после начала мероприятий по митигации рисков (в том числе заключения таких договоров с разработчиками). Фактически вырисовывается следующая ситуация — вскоре после приобретения (консолидации) компанией прав на ПО по относительно небольшой стоимости ее доли продаются по существенно более высокой цене, которая основана на дисконтировании потоков, генерируемых с помощью такого ПО. При этом компания приобрела его «под сделку» в рамках комплекса синхронных операций с авторами по гораздо более низкой цене.

Такие транзакции могут происходить не только между компанией и ее работниками, но и со сторонними разработчиками (которым компания уже ранее выплачивала реальное вознаграждение за разработку ПО), аффилированными структурами и лицами одной корпоративной группы, а также любыми другими категориями субъектов, которые, с высокой вероятностью, являются фактическими текущими правообладателями ПО.

Операции, опосредующие приобретение компанией ключевых активов, в частности, ПО непосредственно перед сделкой по переходу контроля или получения инвестиций, требуют тщательного анализа налоговых последствий для всех участников сделки M&A. Мы попросили налоговых консультантов описать масштаб проблемы и рассказать о возможных налоговых последствиях такой реструктуризации.

[15] В большинстве случаев зрелые компании оцениваются с помощью доходного подхода методом дисконтированных денежных потоков, который может дополняться использованием сравнительного подхода.

#НАЛОГОВЫЕ_ПОСЛЕДСТВИЯ



Андрей Шептий

старший юрист налоговой практикии корпоративного права

VERBA LEGAL

Важно учитывать налоговые последствия при внутригрупповых реструктуризациях посредством «переброски» активов внутри группы. Налоговые последствия здесь могут возникнуть как у компаний, так и у физических лиц.

Например, при определенных условиях у физического лица может возникнуть облагаемый НДФЛ доход в виде материальной выгоды (ст. 212 НК РФ) при приобретении долей участия / акций / товаров по заниженным ценам. У физического лица также может возникнуть налогооблагаемый доход в виде безвозмездно полученного имущества.

При безвозмездной передаче имущества налоговые последствия могут возникнуть и в том случае, если получателем является юридическое лицо (п. 8 ст. 250 НК РФ). При этом существует судебная практика, подтверждающая, что передача имущества по номинальной (кратно заниженной) стоимости может быть переквалифицирована в безвозмездную передачу имущества.

Более того, если передающая сторона безвозмездно передает имущество, реализация которого облагается НДС, то в таком случае НДС будет исчисляться с рыночной стоимости передаваемого имущества (пп. 1 п. 1 ст. 146 НК РФ).

При передаче прав на ПО в рамках реструктуризации потенциально могут возникнуть следующие налоговые риски: (i) налоговые риски в связи с безвозмездной передачей ПО, (ii) утрата права на применение налоговых IT-льгот по налогу на прибыль и страховым взносам.

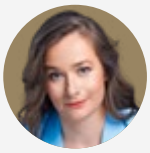
Так, например, при безвозмездном получении прав на ПО в рамках корпоративной реструктуризации у получателя ПО может возникнуть облагаемый налогом на прибыль доход в размере рыночной стоимости безвозмездно полученных прав на ПО (п. 8 ст. 250 НК РФ). Такой доход будет облагаться налогом на прибыль по ставке 25%. Однако если ПО будет передаваться посредством вклада в уставный капитал / имущество, последствия по налогу на прибыль будут отсутствовать.

В связи с этим при структурировании передачи необходимо выбрать наиболее налогово эффективную форму.

Также важно отметить, что применения налоговых льгот по налогу на прибыль и страховым взносам для IT-компаний может быть важно, является ли лицо, генерирующее доход от IT-деятельности, разработчиком ПО или входит ли такое лицо в одну группу лиц с разработчиком ПО. При внутригрупповой передаче ПО необходимо оценить, будет ли выполняться этот критерий после передачи ПО и сможет ли компания применять налоговые IT-льготы.

#МНЕНИЕ_ЛИДЕРОВ_РЫНКА

Налоговые риски предсделочных реструктуризаций и устранения IP-рисков в Tech M&A



Наталья Кузнецова
партнер

O_2 консалтинг

Вопрос о необходимости устранения одного из наиболее чувствительных рисков — неподтвержденности прав на программное обеспечение — остается актуальным для Tech M&A сделок. Несмотря на то, что рынок заметно «повзрослел» и базовая гигиена оформления прав на IP соблюдается все чаще, по нашей практике данный риск по-прежнему выявляется более чем в 50% случаев due diligence.

Как следствие, уже на стадии подготовки сделки возникает задача «сборки» прав на ПО — через отчуждение, дооформление или реструктуризацию владения IP. При такой «сборке» мы сталкиваемся не только со сложностями устранения юридических рисков, но и с налоговыми рисками, возникающими в процессе устранения таких IP-рисков. В условиях повышенного внимания государства к налоговым поступлениям любые операции по консолидации IP перед сделкой рассматриваются сквозь призму ст. 54.1 НК РФ и риска получения необоснованной налоговой выгоды.

На практике это означает, что вопросы налоговой структуризации таких действий все чаще требуют проработки уже на ранних стадиях сделки — вплоть до согласования ключевых подходов на уровне term sheet.

Базовые сценарии устранения IP-рисков

На практике можно выделить несколько типовых ситуаций.

Наиболее «безболезненный» сценарий — когда ключевые разработчики одновременно являются участниками компании или предполагается вхождение этой части команды в капитал перед сделкой с покупателем (например, в рамках реализации опционной программы). В этом случае передача прав может быть структурирована через вклад в уставный капитал или имущество. Такой подход, как правило, минимизирует налоговые риски и позволяет сформировать стоимость доли для целей последующей продажи.

Сравнительно простым кейсом также является дооформление прав по ранее заключенным гражданско-правовым договорам, содержащим указание на разработку для таргета и передачу прав на создаваемые объекты, если суть риска заключается в том, что объект передачи не был надлежащим образом определен. В таком случае при корректном документальном оформлении (допсоглашения, акты) налоговые риски, как правило, являются контролируемыми.

Наибольшую сложность представляют ситуации, когда:

- разработка велась либо вовсе без надлежащего договорного оформления («на словах»), либо на основании договоров без указания на передачу прав;
- трудовые договоры не содержали положений о создании служебных произведений, либо должностные инструкции не предусматривали соответствующий функционал работника.

Устранение юридических рисков в таких кейсах, как правило, сопровождается **наиболее существенными налоговыми рисками**.

Case study: «сборка» IP перед продажей бизнеса

Представим типичную ситуацию, выявляемую при due diligence. Разные части программного продукта (включая функционально самостоятельные модули) принадлежат нескольким правообладателям: физическим лицам (сотрудникам и фрилансерам) и юридическим лицам, часть из которых аффилирована с таргетом.

Для подготовки сделки предлагается консолидировать права на уровне таргета путем заключения договоров об отчуждении исключительных прав с каждым правообладателем. При этом стороны договариваются о передаче прав по символической цене, несмотря на то, что:

- бизнес в целом оценивается, например, в 3 млрд руб.;
- стоимость компании практически полностью обусловлена программным продуктом.

С точки зрения гражданского права такая конструкция реализуема. Однако налоговые последствия делают ее существенно менее тривиальной.

Ключевые налоговые риски

1. **Риски на стороне приобретателя (таргета)**

Основной риск — переквалификация приобретения прав по заниженной цене в безвозмездное получение. В этом случае налоговый орган может доначислить доход в размере рыночной стоимости полученного IP с начислением налога на прибыль.

С учетом того, что стоимость ПО фактически определяет стоимость бизнеса, потенциальные доначисления могут быть сопоставимы с существенной частью цены сделки. Именно этот риск зачастую становится критичным для покупателя.

2. **Риски на стороне «продавцов» (лиц, отчуждающих права на ПО)**

Для юридических лиц — риск доначисления налога на прибыль исходя из рыночной стоимости отчуждаемых прав.

Для физических лиц — риск ниже, но не нулевой, особенно при наличии взаимозависимости или иных признаков контролируемости сделки.

3. **Применение ст. 54.1 НК РФ**

Попытка обосновать деловую цель консолидацией актива перед продажей бизнеса сама по себе не гарантирует отсутствия претензий. Налоговый орган будет оценивать не только наличие деловой цели, но и соразмерность выбранных инструментов, включая ценообразование.

Практика показывает, что наличие деловой цели не исключает переквалификацию операций, если цена существенно отклоняется от рыночной.

Вопрос ценообразования: «символическая цена» как источник риска

Ключевая проблема подобных реструктуризаций — определение стоимости передаваемых прав.

Интуитивное решение «купить за номинал, а затем продать бизнес дорого» практически всегда создает налоговый риск. В глазах налогового органа это выглядит как искусственное занижение стоимости промежуточной сделки.

В этой связи на практике критически важными являются:

- независимая оценка передаваемых прав;
- подготовка защитного файла, обосновывающего подход к ценообразованию;
- анализ вклада каждого модуля в общую стоимость продукта.

Интересный нюанс: если отдельные модули не имеют самостоятельной ценности вне интеграции в единый продукт, это может использоваться как аргумент для снижения их стоимости. Однако такая позиция требует аккуратной экономической и функциональной аргументации.

Можно ли «размазать» риск через структуру сделки?

Теоретически альтернативой является включение всех правообладателей в контур сделки — с выплатой им части общей цены бизнеса.

Такой подход:

- снижает риск налоговых претензий по занижению стоимости;
- но существенно усложняет структуру сделки;
- создает дополнительные юридические и коммерческие риски (множественность сторон, платежная дисциплина, управление потоками).

Поэтому на практике он применяется ограниченно и редко является оптимальным решением.

В целом можно констатировать, что рост сложности предсделочных реструктуризаций в Tech M&A (что подтверждается и результатами отраслевых опросов) во многом обусловлен именно налоговыми аспектами работы с IP.

Это, в свою очередь, приводит к заметному смещению роли налогового структурирования в сделках: если ранее налоговые вопросы зачастую «догоняли» сделку на финальных стадиях, то сегодня они становятся одним из ключевых факторов, влияющих на архитектуру сделки уже на этапе ее проектирования.

И чем раньше компания начинает «приводить в порядок» права на ключевой актив, тем дешевле и безопаснее это обходится — как с юридической, так и с налоговой точки зрения.

Как показали результаты исследования, в практике сопровождения сделок с технологическими активами **сформировался устойчивый подход к управлению рисками** в сделках с технологическими активами. Абсолютное большинство экспертов отметили, что по итогам юридической проверки составляется перечень мероприятий, который позволил бы фактически снизить или полностью устранить выявленные риски. Чаще всего выполнение таких мероприятий начинается до подписания сторонами транзакционной документации. Их перечень в каждой сделке индивидуален и может оказаться весьма объемным. Это напрямую зависит от количества, характера и степени выявленных рисков. При формировании плана таких мероприятий и его реализации следует учитывать их юридическую силу, эффективность и реальную применимость в конкретной ситуации.

При этом многие специалисты разделяют позицию о том, что **большинство рисков, выявленных в рамках юридического due diligence IT-компании, являются принципиально устранимыми**. Для этого приобретаемой компании следует подписать определенные документы, которые бы «довосполнили» пробелы в ее текущих и исторических правоотношениях по поводу разработки и использования IT-активов. Однако некоторые эксперты считают такую позицию излишне оптимистичной. Ведь самые болезненные риски — отсутствие у компании исключительного права на ключевое ПО и сопутствующие ему артефакты (описание архитектуры, техническую документацию, отрицательные результаты тестирования и т. п.) — невозможно устранить за исторический период.

2.4 Договорные механизмы управления рисками

Большинство Tech M&A-экспертов, опрошенных нами в ходе исследования, отметили, что наиболее эффективный подход к управлению рисками в сделках Tech M&A включает следующие опции:

— реализация фактических мероприятий по устранению рисков;

— прямое уменьшение покупной цены на сумму рисков, которые невозможно устранить разумными средствами;

— распределение рисков с помощью договорных инструментов.

Мы попросили ведущих юридических M&A-консультантов рассказать о том, какие договорные механизмы (или их комбинации) распределения рисков в сделках Tech M&A, по их мнению, являются наиболее эффективными.



Арташес Оганов

партнер, глава практики корпоративного права / M&A

sll

Обычно для целей митигации рисков в сделках Tech M&A применяется более-менее стандартный набор защитных инструментов: предварительные условия или условия после закрытия, если по результатам due diligence необходимо исправить какие-либо аспекты, заверения об обстоятельствах, обязательства по возмещению потерь, а также право приобретателя отказаться от сделки в случае реализации риска (как правило, посредством штрафного опциона-пут).

По нашему мнению, наиболее эффективным подходом к митигации рисков является сочетание нескольких инструментов, прежде всего, возмещения имущественных потерь и штрафного опциона. Имущественные потери позволяют заранее зафиксировать сумму возмещения или порядок ее расчета, которые, по общему правилу, не подлежат пересмотру и уменьшению судом, что создает достаточную определенность для обеих сторон сделки в отношении размера компенсации, причитающейся приобретателю в случае наступления негативных обстоятельств. Штрафной опцион же позволяет полностью развернуть сделку и не только вернуть, как минимум, вложения инвестора, а, как максимум, еще и обеспечить ему доходность, которую он должен был бы получить, если бы качество приобретаемого актива соответствовало изначально заявленному продавцом.



Валериан Мамагеишвили

советник

KKMP LEGAL

Среди наиболее результативных механизмов распределения рисков можно выделить корректировку покупной цены и обязательство по возмещению имущественных потерь.

Во-первых, последствия материализации риска могут быть прямо заложены в формулу расчета цены. Такая конструкция позволяет гибко адаптировать экономику сделки под возможные неблагоприятные сценарии. В зависимости от ситуации, риск можно «встроить» в цену двумя способами:

1. Предусмотреть снижение цены за приобретаемую долю, что создает для покупателя право на возврат неосновательно уплаченной части цены при наступлении определенных обстоятельств;
2. Альтернативно — отразить риск в структуре так называемой отложенной цены, то есть в стоимости доли, которую покупатель сможет докупить в будущем, после подтверждения стабильности показателей таргета.

В отличие от заверений об обстоятельствах, данные инструменты не зависят от соблюдения стандарта должной осмотрительности. На практике этот стандарт часто ограничивает возможность эффективно реализовать права по заверениям, особенно при наличии сложных рисков. Поэтому при оценке материальных рисков мы обычно стремимся к использованию механизмов, обеспечивающих более предсказуемое и прямое возмещение, нежели классические заверения, — именно они формируют для покупателя «жесткий» уровень защиты.

Возмещение имущественных потерь

Как отмечает большинство экспертов, опрошенных нами в ходе проведения исследования, наиболее надежным инструментом распределения рисков, выявленных по результатам due diligence, является возмещение имущественных потерь (ст. 406.1 ГК РФ). Он активно используется в сделках с различными типами активов, в том числе с технологическими. Наиболее часто с помощью механизма возмещения имущественных потерь стороны стремятся урегулировать известный им риск, природу и вероятность наступления которого они понимают, в том числе если такой риск стал известен по итогам юридической проверки или процедуры раскрытия информации.

Наличие у покупателя информации о риске препятствует использованию другого инструмента — заверений об обстоятельствах. В силу высокого стандарта осмотрительности инструментарий заверений в случае осведомленности покупателя о рисках будет малоэффективен. Основными преимуществами механизма возмещения имущественных потерь в сравнении с другими средствами компенсационной защиты являются: (i) неприменение стандарта должной осмотрительности покупателя; (ii) возможность обоснования порядка возникновения потерь; (iii) широкая сфера применения.

В сделках Tech M&A с помощью механизма имущественных потерь стороны могут урегулировать широкий набор рисков — от утраты титула на ключевое ПО и датасеты, изъятия у компании серверного оборудования, в памяти которого хранится продукт или отдельные его компоненты, до предъявления третьими лицами претензий в связи с ПО и иными объектами ОИС в составе продукта, киберинцидентами или нарушением требований обработки ПДн.

Обычно продавцы настаивают на том, чтобы требование о возмещение имущественных потерь было подтверждено судом. Чаще всего покупатели соглашаются на это условие, если потери возникли в связи с претензиями третьих лиц. В ходе переговоров между сторонами сделки нередко возникают споры, до какого момента требуется просуживать требования. В большинстве случаев они договариваются о том, что требование должно быть подтверждено вступившим в силу актом суда кассационной инстанции.

Мы попросили участников исследования рассказать, какие подходы к определению размера имущественных потерь (ст. 406.1 ГК РФ) они использовали в 2025 г., выступая на стороне приобретателей технологических активов, в связи с наличием риска утраты титула на ключевое ПО.

#РАЗМЕР_ПОТЕРЬ



Антон Джуплин

партнер

АЛРУД

Стороны согласовывали исключение упущенной выгоды, поэтому расчет потерь сводился к потерям и реальному ущербу через определение расходов на: (i) разработку / создание нового ПО с аналогичным функционалом, или (ii) восстановление стоимости ПО до уровня, как если бы событие для возмещения потерь не наступило, или (iii) приобретение ПО у третьих лиц. Вместе с тем часто возникает вопрос заменяемости ПО. Если ПО незаменяемо (или трудно заменяемо), то риск становится критическим и его размер может приближаться к цене сделки.

#РАЗМЕР_ПОТЕРЬ



Игорь Костенников

советник корпоративной практики

LEVEL Legal Services

По нашему опыту, в том числе в рамках сделок, которые мы сопровождали в 2025 г., выбор конкретного механизма расчета возмещения потерь сильно зависит как от самого актива и того, как он создавался, так и от предпочтений, внутренних политик и требований самого приобретателя.

Наиболее популярным при этом является «комбинированный» подход, в рамках которого используется несколько разных механизмов для расчета потерь. В частности, такая комбинация может включать в себя на альтернативной или в некоторой степени кумулятивной основе рыночную или балансовую стоимость (если актив стоит на балансе по большей стоимости) ключевого ПО, а также расходы, которые необходимо понести для приобретения или разработки нового ПО, которое будет аналогично во всех существенных аспектах утраченному ключевому ПО. Под расходами на разработку аналогичного ПО обычно понимают расходы на написание или переписывание кода, в том числе на найм дополнительного IT-персонала, который может выполнить данную задачу.

Возмещение упущенной выгоды традиционно является менее популярным инструментом защиты интере-

сов покупателя в M&A сделках, однако если покупная цена была рассчитана с «премией» исходя из будущих результатов интеграции продукта в экосистему покупателя, в отдельных случаях такая премия также учитывается для расчета возмещения потерь.

Опциональным элементом имущественных потерь также время от времени может выступать сумма всех понесенных покупателем и / или таргетом расходов, связанных с урегулированием или оспариванием требований третьих лиц, связанных с утратой титула на ключевое ПО и / или с его незаконным использованием.

#РАЗМЕР_ПОТЕРЬ



Софья Смирнова

советник M&A
и корпоративной практики

O_2 консалтинг

По нашему опыту, в практике встречаются различные подходы к расчету размера имущественных потерь, выбор которых зависит от множества факторов, включая порядок коммерциализации ПО, силу переговорной позиции сторон и последующую судьбу приобретаемого ПО в составе бизнеса покупателя. Самым популярным является подход, в котором совмещаются несколько альтернативных вариантов возмещения так, чтобы в конечном счете покупатель получил наиболее полное возмещение. Например, встречался кейс, когда вместе с расходами на «переписывание кода», то есть разработку нового ПО взамен утраченного, покупателю возмещалась сумма «за простой» бизнеса, основанная на убытках, которые компания понесла в связи с нарушением обязательств перед третьими лицами и невозможностью заключения новых контрактов в течение определенного времени. Достаточно сложным аспектом механизма является грамотное исключение «двойного возмещения» в пользу покупателя — продавцу необходимо дать комфорт покупателю так, чтобы не попасть в ситуацию, когда одни и те же экономические потери были бы возмещены продавцом по сути дважды.



Анастасия Духина

старший юрист практики корпоративного права / M&A

sll
SL LEGAL

Подход к определению размера имущественных потерь, как правило, зависит от структуры сделки. В случае, когда приобретатель — финансовый инвестор, приобретший относительно небольшую долю в таргете, имущественные потери более эффективно рассчитываются в привязке к размеру вклада инвестора и общей оценке компании. В то же время если утрата прав на ключевое ПО восполнима, размер имущественных потерь может рассчитываться исходя из рыночной стоимости утраченного ПО и затрат на его замену.

По мнению экспертов, наиболее эффективным подходом к митигации рисков с помощью транзакционных средств является сочетание нескольких инструментов, например, возмещения имущественных потерь, уменьшения покупной цены, а для защиты вложений финансового инвестора — также опциона-пут.

Участники сделок Tech M&A отмечают, что для покупателей активов важно зафиксировать в договоре сумму предвидимых убытков или имущественных потерь с обоснованием порядка их калькуляции. В случае возникновения спора это позволило бы перенести на продавца бремя доказывания убытков меньшего размера. В 2025 г. в этих целях участники сделок стали чаще использовать инструментарий заранее оцененных убытков.

Заверения об обстоятельствах

В целях распределения рисков в сделках с технологическими активами стороны также используют инструментарий заверений об обстоятельствах (ст. 431.2 ГК РФ). В 2025 г. участники сделок все чаще отмечали слабую эффективность этого инструмента и непредсказуемость результата его реализации в судебном порядке. В связи с этим в 2025 г. стороны сделок чаще отказывались от использования заверений в пользу возмещения имущественных потерь, в том числе в отношении рисков, вероятность материализации которых не была высокой, но они имели существенное значение для покупателя. В качестве альтернативного решения участники проектов Tech M&A нередко стремились «продублировать» в заверениях аспекты, которые являются основаниями для возмещения имущественных потерь, с оговоркой об исключении двойного возмещения, а также адаптацией формулировок, исключающих применение подхода «warranty on an indemnity basis».

Ключевыми недостатками использования инструмента заверений являются: (i) высокий стандарт осмотрительности покупателя, квалификация заверений его осведомленностью о рисках, необходмость проведения объемного due diligence; (ii) отсутствие устоявшегося подхода к процедуре и стандартам раскрытия информации продавцом, что создает неконтролируемые риски широкого вменения знания покупателя; (iii) отсутствие единообразной судебной практики по вопросам определения размера убытков.

Наметившаяся в 2024 г. в судебной практике тенденция снижения стандарта должной осмотрительности и отказа от широкого вменения покупателю знания обо всех аспектах деятельности компании по итогам due diligence пока не стала устойчивым стандартом. Поэтому покупатели активов предпочитают перестраховываться и ограничивают использование заверений преимущественно случаями, когда не удалось согласовать более сильный инструмент защиты.

#ЗАВЕРЕНИЯ



Анна Венедиктова

советник

STONEBRIDGE LEGAL

Как правило, ключевое ПО и датасеты охватываются единым термином «интеллектуальная собственность». В отношении них дается стандартный перечень заверений о надлежащем оформлении (приобретении) прав на такие объекты, отсутствии обременений и нарушений прав третьих лиц, должном осуществлении платежей, достаточности таких активов для ведения бизнеса. Кроме того, обычно заверения также направлены на то, чтобы гарантировать способность бизнеса продолжать деятельность независимо от группы продавца и принадлежащих ей прав на ПО.

В зависимости от переговорной позиции покупателя, объем охватываемых заверениями объектов варьируется от преимущественно всех объектов до наиболее существенных.

Для многокомпонентных программ, интегрированных с продуктами и сервисами других правообладателей, запрашивались заверения о надлежащем осуществлении таких интеграций и их соответствии политике правообладателей. Там, где датасеты клиентов являются чрезвычайно значимыми для бизнеса, также обычно обсуждаются вопросы доступа к датасетам, учетным записям клиентов, соблюдения правил использования маркетплейсов приложений (AppStore, PlayMarket и др.).

Широкое распространение получают заверения о включении программ в Реестр отечественного ПО. Прогнозируем, что в связи с созданием с 1 марта 2026 г. Реестра ПО для собственных нужд, Реестра доверенного ПО и Реестра значимых разработчиков тенденции на включение «реестровых» заверений только усилятся.

Заверения нередко «дублируются» основаниями для возмещения имущественных потерь с условием о запрете двойного возмещения. Соотношение заверений с иными средствами защиты во многом зависит от результатов юридической проверки и объемов раскрытия информации. В случае выявления проблем в особенно значимых для бизнеса областях эффективность заверений существенно снижается, поэтому устранение таких дефектов становится предварительным условием для осуществления сделки или основанием для корректировки покупной цены.

Эффективность заверений в сделках cash-in

Большинство сделок с технологическими активами структурируется с использованием элемента cash-in, предполагающим внесение инвестором вклада в уставный и добавочный капитал компании. Как показали итоги проведенных онлайн-опросов, **в 2025 г. формат cash-in являлся наиболее популярным элементом структурирования сделок с технологическими активами**. С высокой вероятностью можно предположить, что такая форма привлечения инвестиций в компании сегмента tech преобладала и в предыдущие годы.

Equity-инвесторы, вкладывающие средства в компанию, стремятся обеспечить такой же уровень договорной защиты своих инвестиций, как и игроки, которые входят в проект с помощью иных механик, например, cash-out или долговых инструментов. В том числе такие участники настаивают на использовании в сделке cash-in инструментария заверений и возмещения имущественных потерь в целях снижения рисков, выявленных в ходе due diligence.

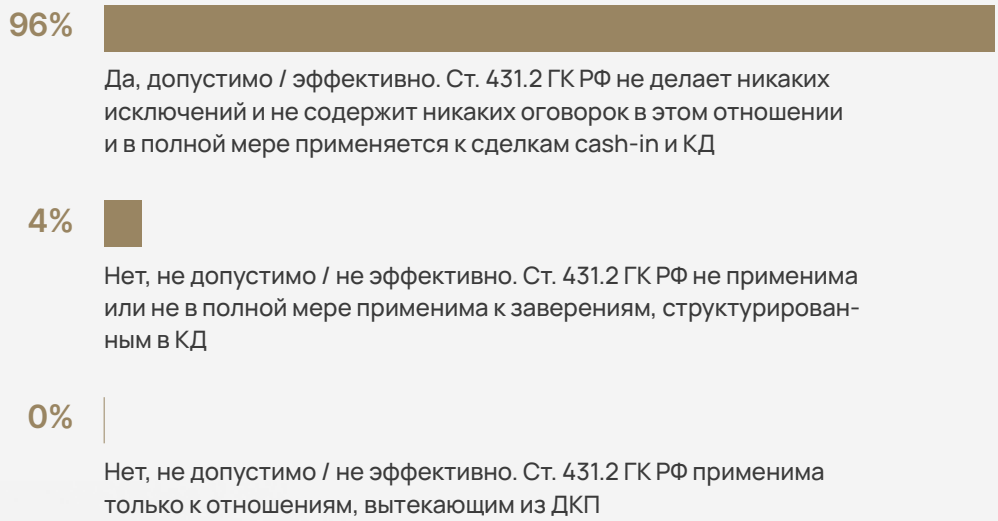
Большинство сделок с технологическими активами заключается в отношении компаний, имеющих форму ООО. Сделка cash-in в ООО оформляется как сочетание корпоративной процедуры увеличения уставного капитала с заключением корпоративного и / или инвестиционного договора. Заверения в пользу инвестора в такой структуре включаются либо в корпоративный договор либо в инвестиционное соглашение, их предоставляет либо участник компании, либо также сама компания. Весь объем договоренностей, оформляющих сделку cash-in, изложенный в указанных документах, может быть квалифицирован как смешанный / непоименованный договор, поскольку вопросы увеличения вклада в уставный капитал и связанные с ними (относящиеся, в первую очередь, к характеристикам бизнеса компании) заверения об обстоятельствах сами по себе не относятся к предмету регулирования корпоративного договора.

В 2025 г. в юридическом сообществе поднимался вопрос о недостаточной эффективности заверений об обстоятельствах при их использовании в рамках структуры cash-in. Среди аргументов были упомянуты: (i) отсутствие четкого предела взыскания убытков, так как сделка cash-in сама по себе не является куплей-продажей и не предусматривает условия о цене; (ii) неопределенность субъекта ответственности по требованию о взыскании убытков в связи с нарушенным заверением — не вполне ясно, кто должен отвечать за нарушение: компания, участник, все участники солидарно и т. п.; (iii) отсутствие судебной практики, подтверждающей возможность взыскания убытков в связи с нарушением заверений об обстоятельствах, включенных в корпоративный договор при оформлении сделки cash-in.

В связи с особой актуальностью данной проблематики и сформировавшейся устойчивой бизнес-практикой включения заверений об обстоятельствах в сделки cash-in, в том числе на уровне КД и инвестиционных соглашений, мы провели онлайн-опрос, посвященный этим аспектам, и попросили ведущих юридических M&A-консультантов прокомментировать его итоги.

#РЕЗУЛЬТАТЫ_ОПРОСОВ

Допустимо ли в сделках cash-in включать в КД заверения участников или компании в пользу инвестора



По данным Опроса об эффективности заверений в сделках cash-in (48 респондентов).

#ЗАВЕРЕНИЯ_В_CASH-IN



Наталья Кузнецова

партнер, руководитель практики M&A и корпоративного права

O2 консалтинг

Сделки cash-in составляют значительную долю сделок в технологическом и IT-секторе. В большинстве случаев, если в сделке участвует фонд или профессиональный инвестор, без предоставления заверений и принятия обязательств возмещения потерь компании, привлекающей инвестиции, и ее основателям не обойтись. На нашей практике включение договоренностей о вносимых инвестициях cash-in, а также заверений и потерь в корпоративные договоры встречается повсеместно и в российском поле очень распространено. Свобода договора позволяет объединять в одном документе разные блоки договоренностей, и суды в рамках корпоративных отношений принимают и понимают такие конструкции.

Попытка направить денежный поток не напрямую в таргет, заинтересованный в инвестициях, в большинстве случаев не обоснована с какой-либо точки зрения. С финансово-экономической это влечет дополнительную налоговую нагрузку на сделку. Так, продавец, получающий cash-out, должен будет сначала уплатить налог на прибыль или НДФЛ с полученного дохода и только после этого остаток вносить в качестве вклада в имущество. Поскольку расходная составляющая почти всегда является несущественной, то при структурировании сделки через cash-out вместо cash-in и при текущих ставках налогов потеря может быть ощутимой по сумме. В сухом остатке таргет получит меньшую сумму инвестиций за счет такой налоговой потери. С юридической — влечет дополнительные риски неполучения средств именно компанией. Не говоря уже о том, что мандаты отдельных фондов могут допускать только сделки cash-in и существенно ограничивать сделки cash-out.

#ЗАВЕРЕНИЯ_В_CASH-IN



Федор Лукьянов

юрист

STONEBRIDGE LEGAL

На нашей практике в случае структурирования сделки по модели cash-in стороны согласовывают корпоративный договор, который подробно фиксирует процедуру увеличения уставного капитала, оценку компании на дату заключения договора, а также, при необходимости, процедуру повторной оценки стоимости компании на дату внесения вклада.

В такой корпоративный договор стороны включают следующие два типа заверений:

1. Заверения в отношении статуса подписантов и действия корпоративного договора, предоставляемые всеми сторонами корпоративного договора: инвестором, текущими участниками и, если стороны согласовывали участие таргета в корпоративном договоре, самим таргетом;
2. Бизнес-заверения в отношении таргета, сопоставимые с типичными бизнес-заверениями в cash-out сделках. Они чаще всего предоставляются инвестору текущими участниками, но не самим таргетом (и для целей исполнимости таких положений стороны дополнительно фиксируют в корпоративном договоре интерес текущих участников в его заключении и предоставлении инвестором вклада таргету). Cash-in типично связан с необходимостью привлечения таргетом финансирования, а дополнительные денежные потери таргета в меньшей степени удовлетворяют интересам инвестора. Инвестор ориентирован на улучшение финансового состояния таргета для возврата своих инвестиций в будущем.

Корпоративный договор обычно предусматривает, что оценка таргета определена с учетом достоверности каждого заверения текущих участников и таргета. В отдельных случаях стороны заранее определяют модель возмещения убытков инвестору. Например, убытки могут рассчитываться как разница между фактическим вкладом и вкладом за аналогичную долю, который инвестор внес бы с учетом недостоверных заверений.

#ЗАВЕРЕНИЯ_В_CASH-IN



Илья Булгаков

советник

DÉNUO

П. 1 ст. 431.2 ГК РФ предусматривает, что сторона, которая при заключении договора дала другой стороне недостоверные заверения об обстоятельствах, обязана возместить другой стороне по ее требованию убытки.

Принцип свободы договора по общему правилу позволяет как включать в один документ неограниченное количество договорных условий, так и помещать каждое такое условие в отдельный договор. Соответственно, один документ (договор) может содержать элементы нескольких сделок и нескольких договоров. По этой причине в корпоративный договор можно включать элементы других договоров и другие договорные условия (как, например, бизнес-заверения относительно самой компании), если это соответствует намерениям сторон.

Кроме того, сама по себе ст. 431.2 ГК РФ не содержит ограничений на то, в какой документ можно включать заверения об обстоятельствах, а в какой — нельзя.

Наконец, если допустить иное толкование, что корпоративный договор не может содержать бизнес-заверения, то получалось бы, что действительность соответствующих бизнес-заверений зависит исключительно от того, в какой документ они помещены, что противоречит как принципу свободы договора, так и в целом диспозитивной направленности гражданского права.

#ЗАВЕРЕНИЯ_В_CASH-IN



Константин Саврыга

юрист

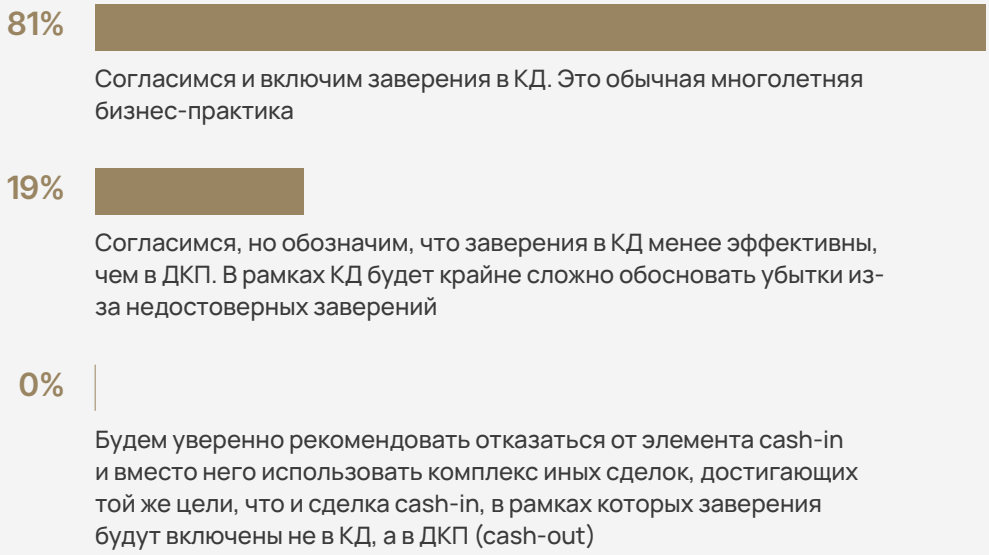
NIKOLSKAYA consulting

Представляется, что нет препятствий для предоставления заверений и индемнити при cash-in как от участника, так и общества. Cash-in в АО оформляется договором купли-продажи при подписке, что снимает большинство вопросов. Cash-in в ООО менее урегулирован, однако нет значимых препятствий к тому, чтобы не считать приобретение доли сделкой, в которой заявление выступает аналогом оферты, а решение о принятии в общество — аналогом акцепта. ВС также прямо указывал, что стороны могут урегулировать договором корпоративные отношениями за пределами императивных норм закона.

Также представляется, что оптимально было бы не включать заверения и индемнити в корпоративный договор, а заключить отдельное соглашение о заверениях и возмещении потерь. Заключение такого договора позволит избежать необходимости воспроизведения исторических положений о заверениях и индемнити при изложении корпоративного договора в новой редакции, а также эффективно регулировать сложные сделки, где cash-in сочетается с cash-out.

#РЕЗУЛЬТАТЫ_ОПРОСОВ #ЗАВЕРЕНИЯ_В_CASH-IN

Если ваш клиент по сделке cash-in попросит включить в КД заверения, как вы поступите?



По данным Опроса об эффективности заверений в сделках cash-in (48 респондентов).

#ЗАВЕРЕНИЯ_В_CASH-IN



Софья Смирнова

советник M&A
и корпоративной практики

O_2 консалтинг

Заверения в корпоративном договоре при cash-in концептуально работают. Это сложившийся рыночный стандарт. Отсутствие «цены» в КД / инвестиционном соглашении не мешает возникновению обязательства между основателями (или обществом) и инвестором: оно рождается из самого факта согласования заверений и возмещения потерь, а взыскивается по п. 4 ст. 431.2 и ст. 406.1 ГК РФ.

Получателем возмещения может быть либо сам инвестор, либо таргет через конструкцию договора в пользу третьего лица (п. 1 ст. 430 ГК РФ), что поддерживается и судебной практикой (например, дело № А40-40990/21 — иск таргета о возмещении убытков из-за недостоверных заверений был удовлетворен полностью).

Размер убытков по умолчанию договорной техникой привязывается к сумме инвестиций. Возмещение убытков настраивается стандартными для M&A договорными механизмами: de minimis, basket, сроки, солидарная или пропорциональная ответственность основателей, выплата инвестору напрямую и / или вкладом в имущество общества, непропорциональное распределение прибыли и т. д.

Таким образом, при надлежащей договорной технике инвестор получает защиту по заверениям и при этом сохраняет главное преимущество cash-in: деньги сразу получает общество, без лишних издержек.

Тем не менее, с учетом сложившегося «пропродавцовского» тренда в судебной практике относительно заверений, а именно ввиду заниженности стандарта оценки того, должен ли был покупатель знать о недостоверности заверений, предпринял ли он все необходимые действия для выяснения их достоверности, справедливым будет отметить и то, что институт возмещения потерь является самым популярным средством защиты покупателя ввиду его относительной понятности в применении. Именно поэтому острота данного фундаментального по своей сути вопроса в юридической практике является не такой заметной.

Поведенческие обязательства

Еще одним неотъемлемым элементом управления рисками на уровне транзакционной документации в сделках Tech M&A являются т. н. поведенческие обязательства продавца в период до и / или после закрытия сделки (pre-closing или post-closing conduct).

Поведенческие обязательства продавца до закрытия сделки играют важную роль в случаях, когда между подписанием и закрытием проходит относительно продолжительный период времени. Чаще всего оценка стоимости бизнеса и акционерного капитала, если применяется механика locked box, завершается гораздо раньше даты подписания[16]. Покупатель оказывается в ситуации, когда он уже принял финансовые и бизнес-риски, отраженные в величине оценки, но к нему еще не перешли юридические инструменты контроля стоимости, так как актив еще полностью находится под управлением продавца. В этот период могут произойти утечки денежного характера (например, вывод дивидендов или выплата бонусов), способные изменить баланс компонентов чистого долга и соответственно итоговую стоимость акционерного капитала (E) по сравнению с той, которая была зафиксирована сторонами до сделки. С уменьшением денежной массы возрастает уровень чистого долга, а значит, итоговая цена должна быть ниже величины, согласованной сторонами по принципу locked box.

Механизм pre-closing conduct является важным юридическим элементом структурирования контроля за утечками стоимости акционерного капитала до закрытия сделки. Если он сопровождается эффективным механизмом мониторинга, позволяющим скорректировать цену на сумму утечек, что объективно является крайне сложным, или сопровожден серьезными санкциями, например обязанностью возместить потери в размере утечек, — это мотивирует продавца и компанию на предотвращение размытия стоимости.

[16] Нередко в рамках использования механики locked box покупатели настаивают на обновлении расчета величин чистого долга и оборотного капитала на дату, максимально близкую к дате подписания документов по сделке, на основании данных управленческой отчетности компании. В некоторых случаях величины чистого долга и допустимые параметры их отклонения фиксируются с помощью инструментария заверений или возмещения имущественных потерь. В этом случае, особенно если сделка закрывается в дату подписания, риск денежных утечек минимизируется.

Даже если стороны договорились об использовании механики completion accounts, ее инструментарий (как и инструментарий механики locked box) не позволяет зафиксировать возможные утечки стоимости бизнеса (EV), так как целеполагание обеих механик — **верификация величин компонентов чистого долга и чистого оборотного капитала, но не стоимости самого бизнеса**. Поэтому в рамках инструментария поведенческих обязательств продавца до закрытия сделки (вне зависимости от эффективности этого механизма, которая небесспорна) важно включать обязательства, **которые также направлены на защиту от размытия стоимости бизнеса**, в первую очередь, от вывода в указанный период ключевых операционных активов, которые лежат в основе показателя EBITDA и действий по перепрофилированию бизнеса.

В частности, стандартной практикой в сделках с технологическими активами является включение в объем обязательств pre-closing conduct требований об обязательном предварительном согласовании с инвестором (особенно стратегическим) сделок, связанных с ПО и прочими ключевыми ОИС в составе продукта, инфраструктурой, заключением или изменением крупных контрактов, сменой вида деятельности и т. п.

Помимо обязательств, направленных на сохранение стоимости компании до момента ее перехода к покупателю, на продавца в рамках транзакционной документации часто налагаются иные обязательства, связанные с завершением мероприятий по митигации рисков, реорганизацей бизнеса, прекращением неиспользуемых товарных знаков или «разделением» бренда, содействием в миграции кодовой базы и пользователей в контур покупателя и т. п.

Объем и состав обязательств продавца после закрытия сделки является также важным элементом регулирования отношений сторон, особенно в рамках структуры earn-out, связанной с высоким риском конфликта мотиваций продавца и покупателя. Такие положения актуальны также и в случаях, если продавец сохраняет участие в компании после первого этапа сделки.

#ПОВЕДЕНЧЕСКИЕ_ОБЯЗАТЕЛЬСТВА



Дмитрий Кажаев

советник

STONEBRIDGE LEGAL

Помимо стандартных для M&A сделок поведенческих обязательств преимущественно негативного характера, подлежащих исполнению продавцом и / или целевой компанией в течение периода до наступления закрытия по сделке и направленных в первую очередь на сохранение имеющегося имущества целевой компании и исключение возможности самостоятельного совершения целевой компанией действий, выходящих за рамки ее обычной хозяйственной деятельности, сделки по приобретению технологического бизнеса зачастую предусматривают ряд активных обязательств продавца и / или целевой компании в отношении используемой ей IT-инфраструктуры, подлежащих исполнению в рассматриваемый период.

Таким образом, наряду с обязательствами по обеспечению отказа целевой компании от отчуждения и / или создания обременений в отношении принадлежащих ей объектов интеллектуальной собственности и сохранения доступа целевой компании к используемой интеллектуальной собственности третьих лиц, в том числе путем продления соответствующих лицензий и обеспечения надлежащих образом контролируемого использования учетных записей на различных цифровых платформах и в социальных сетях и мессенджерах, покупатель может ожидать от продавца принятия последним на себя ряда специфических для конкретной сделки pre-completion обязательств, состав которых обычно формируется по итогам комплексной юридической и технической проверки в отношении целевой компании и может включать, например, обязательства по регистрации прав целевой компании на фактически используемые ей объекты интеллектуальной собственности (или приобретение таких прав у третьих лиц), прекращение незаконного использования объектов интеллектуальной собственности третьих лиц, унификацию используемой IT инфраструктуры в рамках отдельных подразделений целевой компании или членов ее группы лиц и создание — уже на самом раннем этапе реализации сделки — совместного с покупателем комитета по интеграции для выработки и практической реализации сценария бесшовного включения целевой компании в периметр бизнеса покупателя с момента закрытия.

#ПОВЕДЕНЧЕСКИЕ_ОБЯЗАТЕЛЬСТВА



Анастасия Духина

старший юрист практики корпоративного права / M&A

sll
SL LEGAL

Как правило, в перечень действий, которые компания или ее участники не должны совершать до закрытия сделки, распоряжение ИТ-активами и их обременение, прекращение договоров с ключевыми контрагентами, какие-либо действия в отношении ИТ-инфраструктуры, которые могут сказаться на ее работоспособности, а также иные действия и сделки, в зависимости от особенностей бизнеса компании, которые могут негативно сказаться на ее деятельности и показателях.

Раздел 3

Юридический due diligence программных продуктов

Лучшие практики

АВТОРЫ



Анастасия Нерчинская



Александр Панов
VERBA LEGAL



Роман Головацкий
DENUO

Краткие выводы

- ПО и особенно комплексные программные продукты, крайне сложны для юридического анализа в контексте сделок M&A. Проверка таких активов «по существу» требует применения иных подходов, чем те, что используются для анализа других типов активов, например, регистрируемых ОИС или материальных объектов. Ошибки в отношении титула на ключевое ПО могут повлиять на оценку всей компании. Поэтому роль юридической проверки продукта очень велика, а точность ее результатов зависит от правильной организации процесса и приоритизации задач.

- В 2025 г. требования инвесторов к «чистоте» прав на ПО, датасеты и другие ключевые активы приобретаемых IT-бизнесов существенно возросли. Это связано с общим снижением риск-аппетита приобретателей технологических компаний, требованиями к обеспечению соответствия оценки реальному качеству актива, возможности его полноценного развития, сохранению всех заявленных конкурентных преимуществ бизнеса. Титульные риски на ключевые активы не закладываются в ставку дисконтирования и требуют дополнительной проработки в ходе переговоров по итогам оценки и due diligence.

- Многие эксперты отметили, что в 2025 г. глубина и объем due diligence IT-бизнесов увеличились, при этом сроки проверок, на которые влияют коммерческие факторы, преимущественно остались прежними. Процесс проверки IT-активов стал более интенсивным и, соответственно, более сложным как для юридических команд, осуществляющих проверку, так и для команд приобретаемых активов.

- Юридическая проверка прав на продукт проводится в условиях высокой степени «абстракции». В отношении ПО отсутствует система публичной достоверности реестров, продукты часто имеют сложную архитектуру и композицию, их трудно идентифицировать, определить их границы для «документальных» целей, различные компоненты продукта «происходят» из различных источников и имеют длинные цепочки переходов прав. Все эти аспекты крайне затрудняют анализ. Поэтому в процессе юридической проверки важны постоянные кросс-коммуникации со специалистами смежных областей, прежде всего с технической и операционной командами проверяемой компании.

- Коллективная разработка ПО приводит к отношениям соавторства и, соответственно, — со-правообладания. Ошибки на этапе установления соавторства продукта могут стать критичным риском в сделках, структурированных по модели распоряжения правами на весь продукт, в частности, в формате asset-deal. По общему правилу, со-правообладатели совместно распоряжаются исключительным правом на продукт, а доходы от такого распоряжения делятся между ними в равных долях. Если компания в результате дефектов титула окажется одним из со-правообладателей продукта вместе авторами-работниками или третьими лицами, такой риск станет особенно актуальным.

- Оптимальным подходом к организации due diligence зрелых продуктов является их архитектурная декомпозиция и сужение периметра проверки до наиболее значимых объектов и процессов. Критериями значимости отдельных компонентов продукта могут выступать: (i) влияние на финансовый результат (наибольшая доля выручки, эффект снижения расходов, комплементарность и синергетичность продуктам приобретателя); (ii) влияние на параметры работоспособности и безопасности актива в целом; (iii) возможность их оперативной замены, в том числе своими силами, с учетом стоимости приобретения аналога с рынка; (iv) степень вклада ключевых разработчиков в их создание.

- По мнению абсолютного большинства участников сделок Tech M&A, при проверке титула на продукт необходимо анализировать все цепочку переходов прав от первоначальных авторов до текущего правообладателя, не полагаясь лишь на данные свидетельства о государственной регистрации Роспатента. Такой подход является устойчивым стандартом due diligence ПО, отвечающим критериям лучшей рыночной практики.

Для большинства продуктовых компаний ПО является ключевым активом, обеспечивающим существенную часть стоимости бизнеса. При определении оценки IT-компании учитываются риски, с которыми связан приобретаемый актив. Макроэкономические, рыночные (конъюнктурные), валютные (если применимо), страновые, отраслевые, операционные и некоторые специфические риски закладываются в ставку дисконтирования (WACC[17]). Но она **не учитывает юридические риски**, включая те, что выявляются по итогам юридической проверки. Если в отношении ключевого (внеоборотного) актива IT-компании, например ПО, не подтвердится титул, **эта проблема сама по себе не будет учтена в ставке дисконтирования**.

Для целей оценки бизнеса наличие у компании прав на ключевые активы принимается **в качестве предпосылки (допущения) и не верифицируется оценщиком самостоятельно**. По умолчанию оценка производится на основании предположения о том, что компания является правообладателем всех ключевых ОИС, включая ПО, товарные знаки, ноу-хау и другие, и все они находятся в периметре сделки (например, у дочерней структуры основного актива, которая также будет приобретена).

Если по итогам юридической проверки будет выявлено отсутствие титула на ключевое ПО, оценка впоследствии может быть сбалансирована через уменьшение размера потоков / применение дисконта. Однако для такого серьезного шага на стороне продавца потребуется детальное обоснование наличия неустранимого титульного риска в отношении ключевых активов. Документарной верхнеуровневой проверки для этого может быть недостаточно. Это подчеркивает особую роль юридического due diligence ПО и важность его эффективной организации.

[17] Weighted average cost of capital — средневзвешенная стоимость капитала.

3.1 Сложности процедуры due diligence ПО

Программные продукты традиционно являются наиболее сложными объектами с точки зрения их юридического анализа в контексте сделок M&A. Это обусловлено спецификой такого актива, как ПО, форма выражения которого (в первую очередь, исходный и объектный код) не позволяет в полной мере применить к нему классические документарные методы проверки.

В 2025 г. инвесторы стали более строго относиться к качеству юридической проверки IT-активов, особенно в части анализа «чистоты» титул на ПО и крупные массивы данных. Многие эксперты, опрошенные нами в ходе исследования, отметили, что в 2025 г. глубина и объем due diligence IT-бизнесов в целом увеличились, при этом сроки проверок, обусловленные коммерческими договоренностями, преимущественно остались прежними. Процесс проверки IT-активов стал более интенсивным и, соответственно, более сложным как для проверяющих команд, так и для самих компаний, которым приходится выделять ресурс на подготовку ответов и участие в интервью.

В ходе исследования мы попросили Tech M&A экспертов из АЛРУД на примере своей практики рассказать, какие, по их мнению, аспекты юридической проверки программных продуктов являются наиболее сложными и почему.



Сергей Ханаев

партнер

АЛРУД

Наиболее сложными для проверки в юридическом due diligence (DD) становятся следующие вопросы:

1. Прослеживание всей истории создания ПО и соавторов ПО (кем они приходятся для таргета — бенефициарами, работниками, подрядчиками, сторонними разработчиками без договора). Сложность заключается в том, что иногда ПО создается еще до создания таргета, и необходимо определить всех задействованных в создании ПО лиц.
2. Помимо этого, иногда риск может возникнуть только в отношении конкретного ключевого соавтора, когда его вклад в разработку наиболее существенный.
3. В отношении датасетов и процесса сбора данных наиболее сложные вопросы — законность сбора данных и кому принадлежит исключительное право на датасеты как базы данных (если их рассматривать как базы данных).
4. Использование open source-решений, соблюдение лицензий, наличие ограничений, накладываемых open source-лицензиями, и обязательств таргета (например, раскрытие исходного кода, запрет на коммерциализацию). Зачастую требуется участие технических специалистов, чтобы установить степень влияния open source-решений на программный код ПО.
5. Проверка необходимости получения специальных лицензий и разрешений для коммерциализации ПО, например лицензии ФСТЭК для программных средств защиты и обработки информации.
6. Зависимость от интеллектуальной собственности третьих лиц, поскольку информацию о ней возможно получить только напрямую от таргета.
7. Процесс разработки ПО всегда постоянный и итерационный. Зачастую ценность продукта не в первично созданном ПО, а в многочисленных доработках и обновлениях. В этой связи возникают вопросы процесса документального отражения доработок ПО и регулярности этого процесса.

В одном из проектов выяснилось, что все ПО изначально было создано бенефициарами таргета до создания таргета, при этом на момент проведения DD бенефициары уже не принимали участия в разработке. Учитывая данную информацию, критически важным было до сделки организовать отчуждение исключительного права таргету в качестве одного из ключевых предварительных условий для сделки.

В другом проекте выявилось, что в создании ПО принимали участие физические лица — фрилансеры без договора, с некоторыми из которых на момент проведения DD отношения были давно прекращены.

Идентификация и определение «границ»

Юридический due diligence ПО сильно осложняется невозможностью ссылки на какой-либо документ, который мог бы подтвердить наличие у компании прав на программный продукт. В отношении ряда других объектов, например, недвижимости, изобретений, товарных знаков, акций в АО и долей в ООО существует система регистрации прав, позволяющая определить их **текущего титульного владельца и четко зафиксировать «границы» объекта**.

Для ПО такая возможность принципиально отсутствует. Свидетельство о государственной регистрации Роспатента **не обладает свойством публичной достоверности и не позволяет установить правообладателя** ПО. Оно лишь создает предположение в отношении личности правообладателя, которое может быть опровергнуто, в том числе в рамках частноправового спора.

К тому же ПО не является статичным объектом и **постоянно развивается и обновляется**. Версия продукта, которая когда-то могла быть зарегистрирована в Роспатенте, сегодня может **не использоваться** вообще либо оказаться существенно доработанной и **являться уже новым объектом**. Многие продукты, прошедшие процедуру государственной регистрации, не включают последующие критические обновления и не соответствуют текущим характеристикам, на которые ориентируется приобретатель. Также отсутствуют обязательные правила версионирования ПО. Появление новой версии продукта, частота релизов и их содержания — это вопросы маркетинга и стратегии операционного развития.

Поэтому с правовой точки зрения сложно определить, является ли конкретная реализация продукта и его отдельные подсистемы **оригинальным объектом или уже новым — производным от него**. Если речь о производном ПО — важно понимать, в чем заключаются отличия от оригинального и есть ли у компании согласие правообладателя оригинального ПО на создание и коммерциализацию производного. Правильный ответ на этот вопрос имеет важное значение для целей организации юридической проверки.



Мария Ларионова

юрист корпоративной практики и M&A

BETTER CHANCE

Зачастую в юридическом due diligence ИТ-активов сложности могут возникнуть на этапе понимания, что именно является объектом проверки (особенно если не проводилась техническая экспертиза).

Технологические решения, которые продавец или таргет заявляют как ключевые активы, могут находиться на относительно ранних стадиях разработки, быть сложно отделимыми от других объектов или в целом не поддаваться полноценной идентификации. Например, на практике нам встречались случаи, когда на существенные ИТ-активы распространялся режим секрета производства (ноу-хау), что объяснялось невозможностью применить иные режимы охраны интеллектуальных прав в силу особых характеристик объекта.

Кроме того, ИТ-активы — это часто неустойчивые объекты, которые постоянно развиваются, обучаются, модифицируются с привлечением разных команд разработчиков и open source-лицензий. При этом для целей юридической проверки фиксируется некое «статичное» состояние объекта, которое к моменту подписания транзакционных документов уже, вероятнее всего, не будет актуальным.

Все эти особенности могут препятствовать всеобъемлющему изучению ИТ-активов и устранению связанных с ними рисков до сделки, в связи с чем возрастает роль договорных механизмов защиты покупателя — критичное значение получает точность формулировок заверений и обстоятельств возмещения потерь.

В процессе оценки бизнеса наличие у компании прав на ключевые активы принимается в качестве предпосылки (допущения) оценки и самостоятельно оценщиком не верифицируется.

Коллективная разработка и соавторство

Разработка практически любого программного продукта является **коллективной**, а это порождает **отношения соавторства**. Лишь в начале развития продукта его MVP может создаваться единственным автором. Но по мере его совершенствования увеличивается и число разработчиков. В зрелых бизнесах их количество может достигать **нескольких сотен человек**. При этом если сфера деятельности компании не относится к «чувствительной», далеко не все разработчики состоят в штате компании.

Чем масштабнее продукт, тем разнообразнее состав команд разработки его отдельных функций. Это сильно затрудняет корректное установление отношений соавторства, которые неизбежно возникают в процессе разработки.

Один и тот же разработчик может участвовать в создании различных частей и версий продукта, входить во множество рабочих групп, работать в разные периоды, иметь специфические доступы в среды разработки. В зависимости от роли конкретного автора и степени его вклада в кодовую базу, эти аспекты могут оказать большое влияние на корректность выводов по итогам проверки.

Соавторство порождает отношения со-правообладания в отношении созданных ОИС. **Неправильное установление соавторства на продукт может стать критичным риском** в сделках, структурированных по модели распоряжения правами на весь продукт, в первую очередь, — в формате asset-deal. По общему правилу, распоряжение исключительным правом на ПО осуществляется всеми со-правообладателями совместно, а доходы от такого распоряжения делятся между ними в равных долях. Это может оказаться критичным риском. Если компания из-за дефектов титула на отдельные компоненты продукта окажется одним из его со-правообладателей наряду с авторами-работниками или третьими лицами, такой риск станет особенно актуальным.



Софья Смирнова

советник M&A
и корпоративной практики

O_2 консалтинг

На практике достаточно сложно независимо определить список авторов ПО и баз данных, не прибегая к помощи технических специалистов, особенно если разработка не ведется в строгом порядке и документально не фиксируется. Вместе с тем изучение логов в репозитории в отдельных случаях может дать представление об авторах. Поскольку чаще всего ПО пишется в соавторстве, выявление списка авторов часто на практике сопряжено с практическими вопросами о размере творческого вклада тех или иных авторов и размере причитающегося авторского вознаграждения, а также с необходимостью оценки рисков неподписания необходимых документов с бывшими работниками.

Многообразие источников «происхождения» прав на ПО

Еще одно обстоятельство, осложняющее процедуру due diligence ПО, связано с тем, что многие элементы кодовой базы продукта имеют различные источники «происхождения», и, соответственно, к ним применяются **отдельные правовые режимы**, в том числе по-разному регулирующие **момент перехода титула** и необходимые для этого условия.

Например, часть кода продукта пишется разработчиками, состоящими в штате компании. Еще часть ПО компания приобрела по договору об отчуждении исключительных прав у основателей бизнеса, которые начали разработку до создания компании. Другие компоненты продукта могли быть внесены в качестве вклада в уставный капитал технологическим партнером при создании СП. Ряд элементов был создан подрядчиками, среди которых могли быть как физические лица, в том числе не имеющие предпринимательского статуса, так и профессиональные компании-интеграторы. Некоторые ОИС компания могла получить в рамках процедуры реорганизации. Наконец, определенные части ПО могли быть созданы с помощью ИИ-технологий, например, при использовании инструментов вайб-кодинга.

У каждого **охраноспособного** фрагмента исходного кода, которые сначала нужно отделить от неохраняемых, есть свои авторы — физические лица. В рамках юридической проверки необходимо не просто установить «первоисточник» прав на каждый значимый объект в составе продукта, но и проследить всю цепочку переходов прав на него от каждого автора до компании, что является исключительно сложной задачей.



Антон Назаренко

старший юрист практики интеллектуальной собственности

Melling Voitishkin &Partners

Поскольку, как правило, отсутствует единый правоустанавливающий документ, основная задача — найти первоисточник прав на ИС. Эта задача усложняется тем, что ПО практически всегда является результатом кумулятивной разработки нескольких, а иногда и сотен авторов. Отследить участие каждого разработчика и убедиться, что права на все компоненты и версии ПО были должным образом переданы компании, — чрезвычайно трудоемкая задача. Для ее решения требуется очень дотошно подойти к вопросу составления исчерпывающего чек-листа в рамках проверки и подготовки документов по сделке.

Кроме того, процесс разработки ПО детально фиксируется в технических системах: репозиториях кода, таск-трекерах, таких как Jira и т. д. Однако проблема состоит в том, что юридически значимых документов, подтверждающих этот процесс, зачастую нет. Так, если в трудовом договоре обязанность по разработке программ для ЭВМ прямо не входит в трудовую функцию работника, существует риск оспаривания служебного характера ПО и принадлежности прав работодателю.

Этот разрыв между используемыми IT-инструментами и юридической составляющей мог бы быть устранен путем принятия внутренних политик в компании. Например, в политике можно было бы четко прописать, что постановка задачи в Jira является служебным заданием, а загрузка исходного кода в корпоративный репозиторий является частью процесса приема-передачи служебного произведения.



Владислав Лазуткин

старший юрист

ORION

Новый вызов — vibe coding и масштабное использование искусственного интеллекта в программировании, вызванное качественным скачком уровня возможностей ИИ-агентов в 2025 г. Помимо трансформации структуры кода и усложнившейся проверки прав на ПО, меняется также модель работы команд разработчиков и их состав (использовать ИИ для ряда задач может быть экономичнее, чем труд младших программистов).

Прочие основные сложности due diligence ПО: восстановление истории цепочки разработки с учетом отсутствия или наличия какого-либо ее документального оформления и статуса разработчиков, а также анализ системы и процесса постановки задач и формирования результатов.

В одном из кейсов чувствительным фактором стал первичный этап разработки ядра ПО, который осуществлялся с использованием ресурсов европейского партнера на определенных условиях.

Осложняет due diligence ПО и необходимость вовлечения как специалистов по интеллектуальной собственности и трудовым отношениям, так и консультантов по налоговым и коммерческим вопросам: универсальное значение для каждой сделки также имело включение софта в реестр российского ПО и соблюдение соответствующих требований, так как это влияет как на доступ к крупным контрактам в РФ, так и на налоговые льготы / IT-аккредитацию.

Сложная композиция и архитектура продукта

Программные продукты не создаются «с нуля» и включают множество различных «заготовок», «инструментов» и «полуфабрикатов», большинство из которых распространяются по модели open source. В процессе разработки очень востребованы и сторонние проприетарные компоненты ПО, причем использующий их разработчик может заблуждаться в отношении их принадлежности. Например, он может считать их собственной разработкой, а по факту соответствующий фрагмент кода принадлежит его бывшему работодателю, что повлечет риски для всего создаваемого решения, включающего такой компонент.

Большинство программных продуктов являются **сложными программными комплексами**, состоящими из многих десятков модулей, подсистем и классов, что крайне осложняет юридический анализ. Для правильной правовой квалификации важно понимать **архитектурные особенности и композицию** итогового решения, в том числе:

- **общее количество самостоятельных проприетарных объектов ОИС в составе продукта;**
- **характер зависимостей между его ключевыми компонентами;**
- **перечень производного ПО и источники оригинального ПО в составе производного;**
- **список компонентов, разработка которых уже завершена, и тех, которые находятся в процессе разработки;**
- **список компонентов, находящихся в совместной разработке с технологическим партнером, в том числе зарубежным;**
- **перечень наиболее критичных компонентов продукта с точки зрения их влияния на финансовый результат и unit-экономику, работоспособность и безопасность продукта в целом, существенности авторского вклада в их создание, а также стоимости и сроков их замены.**

Эти вопросы следует адресовать технической команде приобретаемой компании в самом начале проверки, как минимум, в формате интервью. Это позволит юристам составить общую картину и сделать юридический анализ более эффективным и сфокусированным. В противном случае проверка будет проводиться «вслепую», без каких-либо материальных ориентиров, что может существенно снизить точность и полезность ее выводов.

> **По мнению большинства экспертов, наиболее сложной задачей в процессе юридической проверки программного продукта является установление и анализ всей цепочки прав — от первоначальных авторов до текущего правообладателя.**

3.2 Лучшие практики организации due diligence программного продукта

Из-за крайней сложности юридической проверки программных продуктов и сжатых сроков сделки у заказчика и исполнителя процедуры due diligence может возникнуть ситуация «разрыва в ожиданиях». Заказчик заинтересован в полноценной проверке и получении точных выводов по ее итогам. Исполнитель, особенно внешний консультант, действующий в условиях информационной асимметрии по сделке в целом, может сделать лишь то, что объективно укладывается в рамки сроков, бюджета проверки и качества исходных данных.

Если заказчик или проверяемая компания не предоставили запрошенные сведения технического и фактического характера, — об архитектуре продукта, составе его авторов, перечне сторонних компонентов и т. п., — эти аспекты юристы самостоятельно установить не смогут. Поэтому консультанты нередко ограничивают свою ответственность на случай таких ситуаций, используя оговорки и допущения о том, что они полагаются на фактические данные, предоставленные компанией, и самостоятельно их не верифицируют. Зачастую это необходимо, чтобы сделать due diligence и не «застрять» на этапе сбора фактической информации.

Для проверяемой компании и особенно заказчика проверки такой подход — это своеобразная зона риска. Если заказчик не прочитает соответствующие оговорки, а консультант не сообщит об ограничениях явным образом, — существует высокая вероятность, что заказчик будет исходить из максимально полной степени проверки всех аспектов, имеющих значение для сделки в рамках согласованного объема. Может возникнуть ситуация, когда в заключении будет написано, что «рисков нет», но не потому, что их действительно нет, а потому, что соответствующие вопросы не анализировались, так как являются предметом исключающей оговорки или следуют из нее.

Чтобы избежать таких ситуаций, следует **максимально прозрачно адресовать заказчику возможные риски, связанные с непредоставлением запрошенной информации** или отказом обеспечить коммуникации с технической и продуктовой командой компании.

В рамках исследования мы провели интервью со многими юридическими командами, сопровождающими проекты Tech M&A, в которых попросили участников поделиться опытом и рекомендациями по организации процесса due diligence программных продуктов. По мнению большинства экспертов, наиболее значимыми этапами, влияющими на эффективность всей проверки, являются следующие:

1. Правильная декомпозиция продукта и фокусировка проверки на **анализе ключевых вопросов**: критичных компонентов, наиболее важных процессов, отношений с авторами, внесшими наибольший вклад в создание ОИС и т. п.

2. Правовая **верификация круга предполагаемых авторов**, установленных технической командой приобретаемой компании, и оценка наличия творческого вклада в созданных ими ОИС.

3. Проверка **всей цепочки переходов прав** на программный продукт и ОИС в его составе, установление принадлежности титула и текущего круга правообладателей продукта.

4. Анализ прочих регуляторных и частно-правовых аспектов. Наиболее значимым областями проверки являются основания **использования сторонних компонентов** ПО, включая open source (также — на основе критерия их материальности для продукта в целом, а для open source — критерия «токсичности») и вопросы **импортозамещения**.

В рамках этих крупных блоков существует множество подзадач. Однако принцип организации работы по **критерию значимости и существенности проверяемых аспектов** позволяет существенно оптимизировать работу в условиях ограниченного времени и бюджета. Его целесообразно придерживаться в рамках всех направлений проверки.

3.2.1 Декомпозиция продукта и приоритизация процесса проверки

Перед командой, осуществляющей юридическую проверку IT-решения, стоят серьезные задачи:

- определить охраноспособные объекты в составе продукта;
- верифицировать круг авторов, оценить степень их вклада в создание ОИС;
- установить хронологию развития продукта и все переходы в цепочке миграции прав;
- проверить наличие у компании титула на продукт и установить круг текущих правообладателей, если таковые существуют помимо компании, включая со-правообладателей;
- проанализировать основания использования продукта в составе ОИС, принадлежащих третьим лицам, включая open source ПО.

Провести такую проверку в полном объеме можно лишь в отношении **небольших проектов**, не имеющих длительной истории. В случае средних и крупных проектов и платформ, разработка которых велась много лет, а число разработчиков и компонентов исчисляется сотнями, такой подход уже не работает. С учетом ограниченных сроков проверки проведение полноценного исследования по таким проектам невозможно в пределах разумного объема привлекаемых ресурсов. Однако именно в средних и крупных проектах от «чистоты» титула и наличия других юридических рисков может существенно зависеть оценка бизнеса и итоговые договоренности по сделке.

> **Любая ошибка, допущенная при определении круга авторов ПО в составе продукта, автоматически ведет к нарушению всей цепочки правообладания или ее соответствующей «ветки». В худшем сценарии авторством или титулом могут быть наделены лица, не являющиеся ни авторами, ни правообладателями. «На бумаге» рисков не окажется, а по факту они сохранятся, но не будут обеспечены транзакционными средствами защиты.**

Фокусировка проверки по критерию материальности

Оптимальным подходом к организации работы со зрелыми проектами является **архитектурная декомпозиция продукта и сужение периметра проверки до наиболее значимых объектов и процессов**. Классифицировать ОИС в составе продукта по степени их существенности для бизнеса может техническая и операционная команда компании с учетом позиции приобретателя, его планов по интеграции и стратегического развития продукта. При определении порога «материальности» компонентов продукта чаще всего учитывается комплекс критериев, в частности:

Влияние на финансовый результат

Определяется, на какие функциональные компоненты продукта прямо или косвенно приходится **наибольшая доля выручки**, какие из них обеспечивают **существенную экономию на расходах**, а также могут быть комплементарны продуктам приобретаемой компании и обеспечить реализацию синергий.

Функциональность

Оценивается, какие компоненты IT-решения носят системообразующий характер и составляют его «функциональное ядро», а какие представляют собой дополнительные опции, в том числе подключаемые бесплатно. Также могут использоваться метрики unit-экономики, показывающие наибольшую LTV отдельных функций, метрики динамики оттока клиентов и отказа от использования продукта в целом при отключении отдельных пакетов функционала.

Безопасность и работоспособность

Определяется, какие компоненты обеспечивают безопасность функционирования продукта (например, модули антифрода, различные фильтры, защита от вредоносного контента и т. п.), а также критически влияют на его работоспособность в целом.

Возможность замены

Устанавливается, какие компоненты можно оперативно заменить аналогом или разработать самостоятельно без ущерба для продукта. Важной метрикой будет определение среднего количества человеко-часов, необходимых на написание соответствующего фрагмента кода, а также возможность и стоимость приобретения аналогов с рынка.

Степень вклада разработчиков

Определяются компоненты, которые разрабатывались авторами, внесшими наибольший вклад в создание всей кодовой базы продукта. Чаще всего такой вклад определяется как доля (в %) строк кода (без учета фрагментов, принадлежащих третьим лицам, включая open source, элементов созданных ИИ и т. п.), созданных конкретным автором, от общего числа строк кодовой базы.

Также определяется доля вкладов каждого автора в создание критичных компонентов, определенных по критериям, изложенным выше. Например, если автор с минимальным общим вкладом в продукт создал 90% одного критичного компонента, его вклад признается значимым.

Одновременно определяется «доступность» таких авторов на момент закрытия сделки, в том числе наличие с ними текущих трудовых или гражданско-правовых отношений.

После определения круга ключевых компонентов, авторов и процессов в отношении них уже проводится полноценная проверка. В то же время нельзя исключить, что даже после такой «фильтрации» общее количество проверяемых объектов все еще будет слишком велико для целей проведения углубленного анализа. В таких случаях потребуется дальнейшее сужение выборки.

#ПРИОРИТЕТЫ_ПРОВЕРКИ_ПО



Мария Мойш

патентный поверенный РФ, старший юрист практики «Интеллектуальная собственность»

VERBA LEGAL

На практике действительно распространен подход, когда в объем юридической проверки входят только ключевые компоненты ПО. Однако открытым остается вопрос определения перечня ключевых компонентов.

Важно также понимать, по каким критериям те или иные компоненты будут отнесены к «вспомогательным» и не подлежащим проверке. Зачастую подразумевается, что такие компоненты можно исключить из состава основного программного продукта без потери его функциональности или заменить их на аналогичные компоненты той же стоимости.

Однако для ответов на указанные вопросы необходимо провести предварительный технический due diligence, который позволит сделать релевантную выборку объектов. Если полагаться только на комментарии со стороны таргета, есть риск получить недостоверную информацию. В результате в объем проверки могут не войти компоненты, имеющие существенное значение для бизнеса компании.

При этом стоит помнить, что даже вспомогательные компоненты могут содержать в себе код, права на который принадлежат третьим лицам. Указанное может повлечь риск взыскания компенсации и запрета использования чужого кода.

Есть нюансы и в случае, когда из объема проверки исключается титул на ПО, зарегистрированное в Роспатенте. Помимо того, что указанная регистрация не носит правоустанавливающий характер, в большинстве случаев задепонированный в Роспатенте код может не содержать важных обновлений ПО, созданных после даты регистрации. Проверить регистрацию на актуальность помогает технический due diligence.

Возможность исключения иных вопросов из объема проверки зависит от особенностей конкретной проверяемой компании. Например, допустимо исключение из проверки титула на ПО, приобретенное на основании договора об отчуждении, если такой договор содержит заверения о чистоте прав.

Вопросы использования открытого / свободного ПО лишь в отдельных случаях могут стать ключевыми. Например, когда компания специализируется на разработке ПО, состоящего из open source компонентов.

#ПРИОРИТЕТЫ_ПРОВЕРКИ_ПО



Илья Булгаков

советник

dénuo

На практике действительно часто проверка ограничивается ключевым ПО, которое непосредственно используется в бизнесе. Однако в вопросе выделения такого ключевого и неключевого ПО потребуется экспертиза технической команды (самого покупателя или привлеченного эксперта). На практике встречаются случаи, когда бо́льшую часть всего ПО можно отнести к неключевому, потому что оно по сути является результатом экспериментов (разработки R&D-департаментов, разработки в рамках правила «20%», когда командам разрешается тратить до 20% своего времени на непрофильные и экспериментальные разработки, спецпроекты для отдельных клиентов) компании и пока не используется таргетом для генерации прибыли. Однако и тут вопрос проверки такого ПО также сложен, потому что крайне сложно определить потенциальное дальнейшее использование такого ПО.

#ПРИОРИТЕТЫ_ПРОВЕРКИ_ПО



Шермет Курбанов

соруководитель практики интеллектуальной собственности и цифрового права

sll
SL LEGAL

@SLLEGAL →

Безусловно, при сделке по покупке IT-таргета программное обеспечение становится одним из наиболее важных объектов проверки. Его уникальные особенности формируют масштаб проверки: объектом может быть как монолитное приложение, так и сложная экосистема из микросервисов, созданных внутренними и внешними командами на разных технологических стеках в течение длительного периода.

При этом, по общему правилу, код — лишь часть ценности. Не менее важными могут быть сохранение ключевых разработчиков, IT-льгот и обеспечение непрерывности бизнеса и работы с контрагентами.

В реалиях сложных сделок с множеством взаимозависимых элементов тотальная юридическая и техническая ревизия каждого элемента сделки часто непрактична. Бизнес вынужден выбирать сфокусированный, риск-ориентированный подход, концентрируясь на наиболее значимых и уязвимых зонах.

Выявление этих точек требует синергии трех экспертиз: бизнеса, юриста и технического специалиста. Именно здесь закладывается фундамент успеха или будущих проблем. Например, элементы технологического стека могут влиять на возможность включения программы в реестр российского ПО, а неучтенная сложность развертывания или миграции инфраструктуры (если необходима) — заморозить интеграцию на месяцы.

Таким образом, качественная подготовительная проверка, организованная как слаженный кросс-функциональный процесс, — это не формальность, а инструмент управления рисками и реализации стратегической ценности сделки.

3.2.2 Верификация авторов продукта

Фундаментальным вопросом, напрямую влияющим на корректность выводов всей юридической проверки продукта, является **правильное установление круга его авторов**. Первоначально титул возникает у авторов, которыми могут быть только физические лица. Поэтому любая ошибка, допущенная на этом уровне, **автоматически ведет к нарушению всей цепочки правообладания** или ее соответствующей «ветки». Как показывает практика, эта проблема серьезно недооценена.

Неправильное определение хотя бы одного автора значимого компонента ПО в составе продукта может привести к пропуску серьезного риска. Если лицо, которое не является автором, будет умышленно или по ошибке «наделено» авторством, и при этом с ним будут впоследствии оформлены правоустанавливающие документы, «закрывающие» риск, проблема все равно остается открытой. Если действительный правообладатель в будущем сможет доказать свое авторство, права на соответствующий фрагмент могут быть оспорены. При этом поскольку в отчете по итогам проверки такой риск указан не будет, соответственно, он не будет урегулирован и защитными механизмами в документах по сделке.

> **Автором может считаться только лицо, чьим личным творческим трудом создан соответствующий объект. Невозможно «назначить» лицо автором, если фактически оно таковым не является, подписав с ним необходимые документы или указав на его авторство в файле кодовой базы. Это может создать ложную «видимость» авторства, но не прекратит авторских прав действительного автора.**

Проблемы определения круга авторов

Правильно определить всех авторов крупного программного продукта — исключительно сложная задача, от которой зависит «чистота» титула.

Первичное определение круга авторов — это предмет экспертизы технической команды. Юристы в абсолютном большинстве случаев **не могут самостоятельно определить авторов ПО**, они могут лишь предположить их состав. В том числе юристы не могут (и не должны) самостоятельно изучать выгрузки из репозитория, в котором хранится кодовая база, и анализировать логи разработчиков.

Обычно такие выгрузки представлены огромными объемами информации, для анализа которых требуется использование программных инструментов или написание специальных скриптов. Делать это «вручную», например на базе excel-файлов, — крайне ресурсозатратная задача даже для проекта, в котором не больше 10 разработчиков, а его продолжительность не превышает года. У большинства компаний, в отношении которых совершаются сделки M&A, гораздо больше и число разработчиков, и продолжительность жизненного цикла продукта, что делает «ручную» проверку всей выгрузки логов из репозитория силами юридической команды неэффективной.

Абстрактное «применение» юридических критериев охраноспособности ПО к конкретным лицам из списка предполагаемых авторов или иное определение авторов «по бумагам» не может достоверно установить факт авторства ПО. Юристы могут лишь сформулировать для технической команды критерии творческого вклада и примерно описать, какие действия и при каких условиях могут привести к появлению охраноспособного результата, а какие — нет. Но установить факт совершения конкретными лицами таких действий юристы самостоятельно не могут. Юридический инструментарий не позволяет этого сделать без первичной фактуры технического характера. Даже подробное интервью с каждым предполагаемым автором, в котором бы «подтвердилось» соблюдение условий творческого вклада, будет лишь косвенным доказательством авторства.

Если список предполагаемых авторов, в том числе сформированный приобретаемой компанией по запросу юридических консультантов, не будет подтвержден, например, с помощью фиксации логов репозитория, с указанием периода разработки, доли вкладов разработчиков в отношении общей кодовой базы, характера коммитов или заключением технического эксперта, — факт авторства конкретных лиц **не может считаться достоверно установленным**.

Некоторые эксперты придерживаются мнения, что даже в ходе технической экспертизы далеко не всегда можно установить авторов с абсолютной степенью достоверности.

#УСТАНОВЛЕНИЕ_АВТОРОВ_ПО



Анатолий Земцов

управляющий партнер

dfcenter

@DFC_BLOG →

В юридическом сообществе существует мнение, что вопрос установления автора такого произведения, как «программа для ЭВМ», может быть разрешен юристами самостоятельно, без привлечения технических специалистов. В каком-то проценте случаев, наверное, да. Но далеко не во всех. Тем более не в тех, где возможны потенциальные риски по этому направлению.

Да, в обоснование такой позиции приводится «сила» свидетельства о госрегистрации программы, внутренние ЛНА компании-работодателя, трудовые договоры, должностные инструкции и так далее. Однако ни один из этих документов не является неопровержимым подтверждением технического факта — кто писал код и что это — код.

Если 15–20 лет назад, а даже тогда — не в 100% случаев, код писался конкретным разработчиком на конкретной локальной ЭВМ работодателя, то сегодня эти процессы часто организованы совершенно иным образом. Помимо вопросов оформления взаимоотношений компании с самим потенциальным автором кода, существует множество более технических вопросов, которыми часто не придают никакого значения при определении автора «по бумагам».

Сегодня кодовая база почти всегда хранится в репозиториях, которых может быть несколько, а находиться они могут не на мощностях работодателя. На кого эти репозитории оформлены, кем оплачиваются — компанией или с личных аккаунтов и карт разработчиков? Как выстроена учетная политика доступа к этим репозиториям — учетки выданы работникам компанией под конкретное ФИО / должность / роль в команде или учетка — это набор символов, причем конкретный владелец учетки никак не определен в контуре компании? Как в случае спора об авторстве будет доказываться, что за конкретной учетной записью был конкретный работник-автор, подписавший документы в части «служебности» произведения? Это прямая угроза в части формирования конечного и прозрачного субъектного состава авторов программы.

Немаловажным является и вопрос разграничения «творческого» и «нетворческого» труда участников разработки. Многие задачи в рамках написания кода — сугубо технические и обусловлены исключительно требованиями используемых при создании программного обеспечения языков программирования или технологий. Их просто нельзя не выполнить, чтобы все «заработало» как нужно. Для решения подобных задач зачастую нужно просто выбрать подходящий вариант решения из конечного количества уже известных. Да, это может быть крайне сложно, для этого требуется высокий уровень знаний и опыта, но творческий ли это труд?

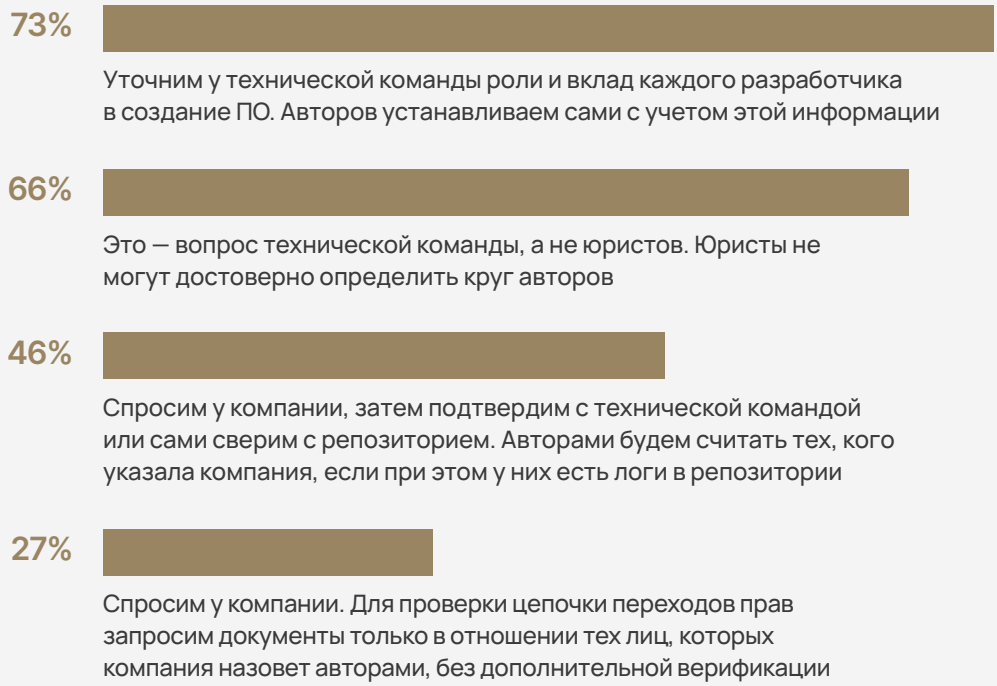
Но даже при наличии действительно уникального «творческого» кода — автором этого произведения может быть не обязательно то лицо, которое внесло этот код в общий программный текст. Или права на этот код этому «автору» не принадлежат. Не говоря про уже общеизвестную проблематику опенсорса, можно выделить, например, действительно авторский код, написанный разработчиком, но написанный в рамках других его проектов для других работодателей (или заказчиков). И права на это произведение он уже передал. Или проблематика ИИ-сгенерированного кода, концепция авторских прав на который сейчас находится в фазе становления, и нельзя однозначно утверждать, кто его автор.

Все эти вопросы объективно невозможно решить только юридическими инструментами, без технических подтверждений и фактологии. Но вместе — эти инструменты дают куда более объективную и твердую позицию.

В ходе исследования мы провели онлайн-опрос, в котором попросили участников отметить, каким образом они обычно определяют авторов ПО в сделках Tech M&A? Результаты приведены ниже.

#РЕЗУЛЬТАТЫ_ОПРОСОВ

Какой подход вы обычно используете для определения круга авторов ПО?



По данным Опроса по аспектам Tech M&A (41 респондент).

Как показали результаты опроса, большинство респондентов (**от 46% до 73%**) при определении круга авторов ПО и других ОИС в составе продукта **обращаются с соответствующим запросом к технической команде**. Это отражает зрелый подход к решению данной задачи и понимание того, что установление авторства — это вопрос факта. Поэтому первичным звеном являются носители технических компетенций.

73% респондентов отметили, что запрашивают у технической команды сведения **о роли и вкладе** каждого разработчика в создание соответствующих фрагментов продукта. По сути такой запрос предполагает проведение технической командой хотя бы поверхностного анализа репозиториев кодовой базы с учетом ее возможных миграций из других хранилищ и сред разработки.

Описание **роли потенциального автора** может существенно помочь юристам в анализе творческого характера его вклада. Например, full-stack разработчик с большей вероятностью может признаваться автором, чем отладчик или «владелец продукта» (product owner). А позиция архитектора ПО для целей определения авторства может потребовать более тщательного анализа созданных им артефактов. При этом гипотетически каждый из них может иметь доступ в одни и те же среды разработки.

Что касается **вклада в разработку продукта**, важны сведения о долях (в %) строк кода, созданных разработчиками, от общего числа строк кодовой базы, а также о долях их вкладов (оцененных в % относительно общего числа строк кода в таких компонентах) в крупных структурных частях продукта. Общее число строк кода или коммитов (в абсолютном выражении), созданных разработчиками, само по себе менее информативно. Объем коммитов, как и их число, могут быть совершенно разными, поэтому эта информация носит лишь второстепенный характер.

46% респондентов отметили, что считают оптимальным гибридный подход к определению круга авторов, при котором учитываются сведения из разных источников. В первую очередь, — от самой компании (это может быть как бизнес-команда, так и непосредственно сами разработчики), а также от команды приобретателя (в том числе привлеченных им технических экспертов). При этом юристы гипотетически готовы самостоятельно сверить предоставленный список авторов с логами из репозиториев. Это не будет лишним, если такие данные подтверждают первичный список. Однако если, по данным репозитория, круг потенциальных авторов окажется шире, юристам не следует самостоятельно включать их в перечень авторов без дополнительной проверки. Наличие у лица доступа в репозиторий само по себе не делает его автором.

Подход, в соответствии с которым юристы при определении авторства полагаются лишь на данные, предоставленные компанией(его отметили **27% респондентов**), не является удачным решением. Компания может не знать критериев охраноспособности ПО и других ОИС и указать авторами лиц, которые таковыми могут не являться. В этом случае итоги проверки могут оказаться некорректными.

#УСТАНОВЛЕНИЕ_АВТОРОВ_ПО



Роман Головацкий

партнер

dénuo

Применяемая методология оценки круга авторов может быть разной и выбирается с учетом ряда факторов, в том числе с учетом объема команды разработки, длительности разработки, зрелости процессов управления исходным кодом, доступности документации, а также бюджета и сроков проверки.

Так, в отношении компаний с небольшим или относительно небольшим количеством разработчиков проверка может быть не только документарной, но и включать техническую валидацию участия конкретных лиц в разработке, в том числе оценку логов в репозиториях, истории коммитов, оценку роли и вклада каждого разработчика. В случаях со сложными многокомпонентными программными продуктами со множеством авторов и в условиях ограниченных сроков такая проверка может быть очень времязатратной и ресурсоемкой, и в таких ситуациях клиенты чаще предпочитают ограниченный формат проверки.

Однако необходимо понимать, что любой из применяемых на практике подходов не является стопроцентно надежным, поскольку так или иначе многое зависит от качества информации, предоставляемой таргетом (по количеству и кругу разработчиков, по соответствию аккаунтов в репозиториях, с которых делаются коммиты, конкретным лицам, по количеству используемых репозиториев и т. д.). Соответственно, выводы в любом случае формулируются с учетом указанных ограничений.

#УСТАНОВЛЕНИЕ_АВТОРОВ_ПО



Алексей Дарков

советник, руководитель практики «Интеллектуальная собственность»

VERBA LEGAL

Практика определения круга авторов ПО при due diligence показывает, что даже у профессиональных игроков нет единого стандарта. По сути компании балансируют между двумя крайностями: максимально погружаться в фактическую сторону вопроса (анализ вкладов каждого разработчика, репозиториев, кода) либо полагаться на заверения самой приобретаемой компании. Выбор стратегии определяется по итогам первичного предоставления информации со стороны таргета на предоставленный запрос информации.

Главный вызов здесь в том, что авторство — это вопрос факта, а не права. Юристы могут оценить документы и договоры, но установить, кто именно создал тот или иной фрагмент кода, без участия технической команды невозможно. Поэтому на практике, безусловно, хорошо использовать гибридный подход: юристы фиксируют критерии верности оформления отношений с действительными авторами, а технические эксперты помогают определить перечень и зоны ответственности ключевых сотрудников. Чего действительно не хватает зачастую, так это взаимодействия между внутренней командой технического аудита и внешней юридической командой. Потому что в IT технический аудит, как правило, касается «бизнеса», а юридические вопросы зачастую считаются формальностями. Поэтому даже при применении гибридного формата отсутствие взаимодействия между командами может лишать проверку хорошего инструмента в части валидации перехода прав от авторов, действительно причастных к написанию кода.

Интересно, что в последние два года в эти процессы добавился еще один фактор — использование ИИ при разработке. Вопрос о том, может ли фрагмент кода, сгенерированный машиной, считаться результатом творческого труда конкретного человека, пока не имеет однозначного ответа в российском праве. Определенное время эта ситуация будет находиться в серой зоне. Но по сути она ничем не отличается от ситуации,

когда права на код оформляются на одного или нескольких разработчиков, а часть уволившихся сотрудников или внешних подрядчиков так и остаются без надлежащих документов с таргетом.

#УСТАНОВЛЕНИЕ_АВТОРОВ_ПО



Софья Смирнова

советник M&A
и корпоративной практики

O_2 консалтинг

Мы полагаем, что в этом вопросе справедливо и экономически оправданно распределить ресурсы команды комплексной проверки, что техническая команда определяет круг авторов и оценивает степени их творческого вклада (на основе первичного опросника от юристов), а затем предоставляет данные юридической команде для оценки рисков (согласились с этим 66% респондентов). Действительно, юристы хоть и являются конечной точкой, определяющей наличие или отсутствие того или иного риска, достоверно установить тот или иной факт должны профессионалы (с соответствующим руководством). Вместе с тем при отсутствии в команде технических специалистов юристы, специализирующиеся в проверках ИТ-бизнеса, способны проявить должный уровень погружения, чтобы оценить наличие логов в репозиториях, сопоставить его со списком авторов, оценить роли авторов через призму технического устройства объекта, не погружаясь детально в, скажем, программный код. Совершенно ясно одно: данный вопрос ни в коем случае не может остаться без внимания юристов и не может быть отдан на откуп исключительно словам таргета о списке авторов или списку действующих работников компании-таргета.

#УСТАНОВЛЕНИЕ_АВТОРОВ_ПО



Кирилл Колесников

ведущий юрисконсульт практики интеллектуальной собственности

ЭБР
Юридическая Компания

Результаты опроса показывают, что большинство респондентов устанавливают авторов по итогам общения с технической командой — 73%. Этот подход позволяет юристам на основании полученной информации оценить, действительно ли конкретный член команды внес творческий вклад в создание программы. С одной стороны, это крайне удобно для юристов, т. к. им остается лишь выбрать авторов исходя из предоставленного списка. С другой стороны, это также удобно и самой компании, т. к. ей необходимо лишь предоставить информацию.

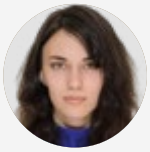
Вместе с тем у такого подхода есть очевидный недостаток. Если кто-то из технической команды ошибся или забыл указать одного из участников (а такое может быть, если разработка велась не 1 год), это может фактически свести результаты проверки на нет. Аналогичный недостаток есть как и у второго, так и у наименее популярного вариантов ответа: когда установление авторов полностью относится к зоне ответственности технической команды (66%) или когда авторов указывает сама компания (27%).

Наиболее проработанным выглядит подход, при котором сначала запрашивается информация у компании, а затем проводится проверка репозитория: у кого есть логи, тот и рассматривается как автор. Такой вариант выбрали 46% респондентов.

Однако и у этого подхода есть ограничение: он не учитывает в качестве соавторов лиц, которые не разрабатывали исходный код, например архитекторов, аналитиков и иных членов команды. Судебная практика по признанию таких лиц соавторами неоднозначна, но полное игнорирование их возможного вклада создает неоправданный риск.

Как итог: полностью устранить все риски невозможно. Однако наша практика показывает, что максимально приблизиться к этому можно, если при проверке проводится полноценное интервьюирование технической команды, а также анализируются репозиторий и система постановки задач. Только сочетание этих подходов позволяет минимизировать риски инвестора при покупке компании.

Какие сведения следует запросить у технической команды



Анастасия Нерчинская

До начала юридической проверки программного продукта у технической команды компании полезно запросить следующую информацию:

1. **Описание и тип архитектуры продукта**

   с указанием структурных компонентов (модулей, подсистем, классов), способов их линкования, сред развертывания, их функциональности. Это позволит юристам лучше понять структуру продукта в целом и применить к нему соответствующие правовые режимы, определить периметр собственной разработки и области использования готовых программных компонентов, выступающих в качестве ресурса.

2. **Период жизненного цикла продукта**

   с разбивкой по основным стадиям — например, прототип, MVP, новые версии, содержащие критические обновления. Эти сведения помогут определить хронологию создания продукта и соотнести с ними сведения из документов, на основании которых велась разработка, включая периоды работы конкретных авторов и т. п.

3. **Перечень лиц, имеющих доступ в информационные системы и среды разработки,**

   с указанием:

   - их роли в проекте (frontend / backend / full-stack разработчик, дизайнер, архитектор, тестировщик, отладчик и т. д.);
   - логина / никнейма в средах разработки;
   - дат приема на работу, заключения гражданско-правового договора или начала фактической работы (если нет договора); дат окончания работы / увольнения;
   - объема кода, созданного каждым из них (например, % коммитов в репозитории), если применимо;
   - описание конкретного вклада в разработку продукта каждого из таких лиц, а также иных лиц, в том числе не имевших доступа в информационные системы, с указанием, кто из них:
     - придумал идею или концепцию продукта, его функционал, маркетинговые характеристики;
     - разработал его архитектуру;
     - непосредственно писал код;
     - создавал элементы дизайна;
     - подбирал компоненты / средства для линковки и интеграции;
     - управлял процессом разработки.

Это поможет юристам верифицировать первоначальный круг авторов продукта, определенный командой, сверить цепочку переходов прав с ключевыми этапами его создания, что позволит сделать более точные выводы о принадлежности титула.

4. **Структура команды разработки и описание процесса взаимодействия**

   внутри нее при создании или модификации продукта: этапы разработки, тестирования, отладки, рефакторинга, загрузки / выкладки кода в мастер-версию кодовой базы.

Это поможет верифицировать круг авторов продукта. Например, если за младшими разработчиками код проверяют старшие, после чего они выкладывают код в «мастер-ветку» — далеко не всегда старшие будут считаться авторами соответствующих фрагментов, хотя объем

таких коммитов может быть большим. Если ошибок в коде не было или они были несущественными, не требующими создания нового кода, старший проверяющий разработчик может вообще не являться автором этого фрагмента. В остальных случаях он может быть соавтором. Однако по умолчанию в мастер-версии логи будут показывать только старшего разработчика. Поэтому чтобы исключить ошибку в авторстве, данные репозиториев следует сверять с другими сведениями о процессе разработки.

5. **Описание информационных систем, используемых при разработке ПО**:

   системы контроля версий, репозитории / хранилища кодовой базы, трекинговые системы, мессенджеры, почта, и т. п. Это позволит понять, как фактически организован процесс разработки продукта и получения обратной связи, ведется ли разработка преимущественно в электронной среде или «на бумаге», как работники получают задания по разработке, интегрированы ли хранилища кода с трекинговыми системами и т. п. Если процесс разработки не закреплен в ЛНА и трудовых договорах — это может привести в будущем к спорам о том, кто из разработчиков какие артефакты сделал, в какой срок, состоялся ли факт их «физической» передачи работодателю и т. п.

6. **Перечень критичных компонентов ПО**

   (например, подсистем, на функционал которых приходится большая часть выручки, или которые наиболее комплементарны продуктам приобретателя и могут стать источником синергии, или при выходе из строя которых блокируется или становится уязвимой работа всего продукта). Это поможет расставить приоритеты при организации проверки и оценке рисков.

Ошибки при установлении круга авторов

Наиболее распространенной ошибкой в процессе определения авторов является их первичный «поиск» исключительно на основе документов, в которых они могли быть упомянуты. Немало специалистов начинают юридическую проверку с запроса и анализа имеющихся у компании документов, которые касаются разработки ПО, а не с установления фактических обстоятельств авторства. Лиц, которые указаны в таких документах, они автоматически признают авторами.

Во-первых, такой подход сужает потенциальный круг авторов. Он основан на допущении, что отношения по разработке были документально оформлены со всеми без исключения авторами ПО, что бывает далеко не всегда.

Во-вторых, такой подход не гарантирует авторства лиц, упомянутых в качестве разработчиков в соответствующих документах — договорах, актах или счетах. Физическое лицо, указанное исполнителем в договоре на разработку, может не являться непосредственным автором ПО.

ТОП-5 распространенных ошибок при определении круга авторов ПО

Неверно полагать, что по умолчанию автором ПО является какое-либо лицо только на основании того, что оно:

- придумало идею или концепцию программного проукта, его структуру и функционал, принципы работы и возможности монетизации;
- имеет учетную запись в репозитории или доступ к иной среде разработки;
- вносило коммиты в репозиторий;
- является генеральным директором компании или иным топ-менеджером, в том числе CTO, если в его должностные обязанности не входит разработка ПО;
- делало отладку, тестирование, устранение ошибок в коде, состояло в рабочей группе по разработке ПО.

Эти обстоятельства сами по себе не являются «гарантией» авторства и требуют дополнительной верификации.

3.2.3 Проверка цепочки переходов прав на ПО

Важнейшим этапом юридической проверки продукта является правильное установление всей цепочки (а точнее, всего их многообразия) переходов прав на ПО и прочих ОИС в его составе, включая архитектуру, техническую документацию, предыдущие версии продукта, результаты тестирования, объекты графики и дизайна, аудиовизуальные элементы. С учетом множества источников «происхождения» прав на ПО и другие ОИС, большого числа их авторов, многослойности процесса разработки, сделать это правильно — крайне сложная задача, требующая высокого уровня экспертизы.

Права на все т. н. «предыдущие версии» также важно включить в периметр проверки и «забрать их» в сделку, несмотря на то, что текущая версия продукта может быть сильно переработана по сравнению с более ранними.

Во-первых, сохранение контроля у продавца над предыдущими версиями ПО может создать риск утраты конкурентных преимуществ. Они отражают результаты «проб и ошибок» при создании текущей версии, что само по себе может иметь ценность для создания конкурирующего продукта.

Во-вторых, текущая версия продукта может быть производна от предыдущих и иметь в основе их охраноспособные части, в отношении которых целесообразно получить полный титул и не зависеть от продавца.

> **Проверку прав на продукт следует начинать не с изучения имеющихся документов, а с установления фактических обстоятельств авторства и определения авторов. Проверка «по документам» — это следующий шаг. Полагаться только на документарный подход — ненадежно. Фактический круг авторов может быть как шире, так и уже круга лиц, указанных в документах компании.**

Проверка «чистоты» титула на продукт **требует анализа всей цепочки переходов прав**, начиная от создания первых фрагментов ПО до текущего состояния продукта. Для этого важно правильно определить хронологию разработки продукта. Неверно начинать отсчет жизненного цикла ПО с момента создания компании, если основная разработка проводилась на базе ее ресурсов. Часто разработка начинается до создания юридического лица либо в период трудоустройства первого автора в другой компании.

Как уже отмечалось ранее, при проверке титула на продукт не следует ограничиваться анализом сведений о правообладании и авторстве, указанных в свидетельстве о государственной регистрации ПО. На практике такой подход нередко используется с целью экономии времени. Основным аргументом в его защиту выступает ссылка на его допустимость судебной практикой. Действительно, существует немало споров, в рамках которых титул на ПО подтверждался именно свидетельством о регистрации, поскольку презумпция авторства не была опровергнута. Ее опровержение требует крайне сложной работы по формированию доказательственной базы. В этом смысле свидетельство может иметь важное процессуальное значение, поскольку **помогает перенести бремя доказывания на другую сторону**. Но это не означает, что в силу этого вопрос о титуле исчерпывается.

Свидетельство о государственной регистрации Роспатента создает лишь опровержимую презумпцию принадлежности прав и авторства. Его наличие само по себе **не может заменить полноценную проверку титула в рамках процедуры due diligence**. Эту позицию разделяет абсолютное большинство участников сделок Tech M&A, включая IT-юристов, которых мы попросили прокомментировать соответствующий вопрос. По мнению экспертного сообщества, такой подход рассматривается ими не как факультативный, а как устойчивый стандарт due diligence ПО, отвечающий критериям лучшей рыночный практики.

#АНАЛИЗ_ЦЕПОЧКИ_ПРАВООБЛАДАНИЯ



Булат Жамбалнимбуев

партнер и руководитель корпоративной практики

NEXTONS



Ксения Михайлова

советник корпоративной практики

NEXTONS

В Tech M&A сделках мы проверяем титул на ПО полностью, так как это основной актив в приобретаемом бизнесе. Мы не ограничиваемся анализом данных о государственной регистрации, поскольку они не гарантируют чистоту титула и отсутствие прав третьих лиц.

Наша проверка достаточно обширна и включает в том числе:

1. Проверку договоров с разработчиками (трудовые, гражданско-правовые);
2. Анализ первичных документов (акты, технические задания, служебные задания);
3. Оценку корпоративных документов (локальные акты, должностные инструкции);
4. Исследование всей вертикали договоров (при наличии цепочек передачи прав).

Отсутствие у компании титула на ПО может привести к целому ряду последствий:

1. Риск остановки бизнеса: автор-разработчик (правообладатель) может запретить использование ПО, что парализует основной продукт компании;
2. Финансовые потери: взыскание убытков и компенсаций за незаконное использование со стороны авторов-разработчиков (правообладателей);
3. Репутационные и договорные риски: невозможность исполнения обязательств перед клиентами, ведущая к искам о возмещении вреда;
4. Риск нереализации сделки: обнаруженные проблемы с титулом могут сделать актив непередаваемым;
5. Риск привлечения к ответственности: компания и ее должностные лица могут быть привлечены к административной и уголовной (применительно к физическим лицам) ответственности.

Таким образом, только всесторонняя проверка ПО позволяет оценить реальную стоимость актива, структурировать сделку и защитить интересы инвестора от скрытых юридических рисков.

#АНАЛИЗ_ЦЕПОЧКИ_ПРАВООБЛАДАНИЯ



Сергей Ханаев

партнер

АЛРУД

АЛРУД не опирается только на государственные реестры, поскольку они не могут в полной мере подтвердить принадлежность таргету исключительного права на ПО.

АЛРУД анализирует всю цепочку создания ПО, начиная с того, создавалось ли ПО уже после создания таргета или до его создания. Анализируется состав авторов ПО (учредители, работники, подрядчики, лица без договоров, иные общества группы (и их работники)), обеспечение режима служебных произведений ПО у таргета, наличие лицензий на использование стороннего ПО в составе ПО таргета.

#АНАЛИЗ_ЦЕПОЧКИ_ПРАВООБЛАДАНИЯ



Мария Баева

партнер, корпоративная практика, глава коммерческой практики

LEVEL Legal Services

При сопровождении M&A сделок с программным обеспечением в качестве ключевого актива таргета критически важно проверять всю цепочку перехода исключительного права от первоначального автора к таргету, а не ограничиваться формальной проверкой сведений о государственной регистрации.

ПО является объектом авторского права и в соответствии с российским законодательством не подлежит обязательной государственной регистрации. В отличие, например, от объектов патентного права, возникновение и принадлежность исключительного права на ПО не зависят от регистрации в реестре Роспатента или Минцифры. Такая регистрация носит факультативный характер и не является гарантией наличия исключительного права у заявителя. Регистрирующий орган не исследует основания возникновения права, не проверяет договоры с авторами, а также правомерность перехода исключительных прав к заявителю. Соответственно, свидетельство о регистрации подтверждает лишь факт внесения сведений в реестр, но не является правоустанавливающим документом и не исключает претензий со стороны третьих лиц, включая разработчиков и бывших работодателей.

#МНЕНИЕ_ЭКСПЕРТОВ

Показательным примером является сделка по приобретению американской компанией F5 Networks стартапа NGINX Inc. за 670 млн долл. Через девять месяцев после закрытия сделки холдинг Rambler Group потребовал признать себя правообладателем исходного кода, обосновывая претензию тем, что создатель веб-сервера NGINX разрабатывал первые версии программного обеспечения, будучи сотрудником Rambler Group. В ходе due diligence не была проверена вся цепочка перехода прав, в результате чего риск возможных претензий бывшего работодателя остался невыявленным. В итоге выгодная (на первый взгляд) сделка стала источником значительных убытков и судебных разбирательств.

Этот пример наглядно демонстрирует, что комплексная проверка цепочки перехода прав от автора исходного кода к таргету — это не формальность, а необходимое условие защиты интересов покупателя.

#АНАЛИЗ_ЦЕПОЧКИ_ПРАВООБЛАДАНИЯ



Алексей Мустяца

директор, управление слияний и поглощений

СОВКОМБАНК

Определение круга авторов и проверка титула осуществлялись по всей цепочке создания и отчуждения прав с использованием кадровых и договорных документов, а также данных технического аудита (репозитории, архитектура кода и т. д.). Государственная регистрация ПО рассматривалась как вспомогательный элемент и не заменяла полноценной проверки прав.

#АНАЛИЗ_ЦЕПОЧКИ_ПРАВООБЛАДАНИЯ



Владислав Абрамов

директор по правовым вопросам

KAMA FLOW

Мы осуществляем проверку титула на программное обеспечение в полном объеме, то есть анализируем всю цепочку прав, а не ограничиваемся только сведениями из свидетельств о государственной регистрации или государственных реестров. Это связано с тем, что регистрация или внесение в реестры само по себе не гарантирует наличие полного и бесспорного правового титула. Комплексная проверка позволяет выявить возможные ограничения, обременения прав, условия лицензионных соглашений, а также случаи перехода прав, что критически важно для минимизации юридических рисков при использовании или приобретении ПО.

#АНАЛИЗ_ЦЕПОЧКИ_ПРАВООБЛАДАНИЯ



Софья Смирнова

советник M&A
и корпоративной практики

O_2 консалтинг

Представляется критически важным проверять всю цепочку перехода исключительного права на ПО как ключевой актив, без которого невозможно определить подлинную стоимость бизнеса. Сама по себе регистрация факта принадлежности прав на программы для ЭВМ в государственном реестре не является защитой от предъявления требований третьих лиц. В частности, регистрация права на программу за работодателем не будет играть определяющей роли в спорах о праве между бывшим работником и работодателем ввиду отсутствия у произведения статуса служебного. Важно понимать, что наряду с вопросами о принадлежности исключительного права на ПО тому или иному лицу встают вопросы о возмещении (убытков, компенсации, авторского вознаграждения) — то есть таргет может понести существенные материальные расходы. Наконец, репутационные потери при возникновении подобных споров также могут быть существенны как для таргета, так и для покупателя. Надлежащая проверка титула на ПО может помочь идентифицировать ключевые рисковые области и вовремя принять все необходимые превентивные меры (как до сделки, так и после сделки).

#АНАЛИЗ_ЦЕПОЧКИ_ПРАВООБЛАДАНИЯ



Владислав Лазуткин

старший юрист

ORION

Анализируем всю цепочку разработки и оформления, разумеется. Одна лишь формальная проверка вопросов регистрации / депонирования ПО не подразумевает проверку рисков, связанных с титулом по существу.

#АНАЛИЗ_ЦЕПОЧКИ_ПРАВООБЛАДАНИЯ



Тигран Микаелян

юрист корпоративной практики

ELWI

Мы (или в отдельных случаях внутренняя команда покупателя, обладающая необходимой экспертизой) практически всегда проводим полную проверку всех необходимых документов, связанных с созданием и подтверждением прав на основное ПО таргета, включая положения трудовых договоров о правах на служебное произведение, договоры с лицензиарами, служебные акты и расчеты по соответствующим сделкам. С учетом того, что внесение ПО в государственные реестры не гарантирует отсутствие рисков в отношении титула на ПО, являющееся ключевым активом приобретаемого бизнеса, проверка свидетельств о государственной регистрации является недостаточной. Такой подход предоставляет следующие возможности:

- идентифицировать риски, которые могут оказать существенное влияние на оценку бизнеса и принятие решения о вхождении в сделку;
- в той мере, в какой это возможно, «вылечить» отдельные риски до закрытия сделки в рамках отлагательных условий;
- заранее наметить отдельные мероприятия по изменению внутренних документов и практики приобретаемой компании по заключению соответствующих договоров в отношении ПО.

Ошибки при проверке цепочки правообладания

Наиболее сложной частью юридической проверки продукта является анализ отношений с разработчиками и восстановление всей цепочки правообладателей. Именно на этом этапе возникает критическая масса ошибок, приводящих к неверным выводам по итогам проверки. Далее описаны наиболее распространенные из них:

- **Неверно установлен круг авторов продукта**

  Это автоматически ставит под сомнение всю последующую цепочку переходов прав.

- **Неправильно квалифицированы правоотношения с разработчиками**

  Не все договоры соответствуют своему названию. За формальным «отчуждением прав» может скрываться лицензия (для этого достаточно пропустить упоминание об отчуждении в прав «в полном объеме»), подряд, оказание услуг, заказная разработка либо смешанная конструкция. Поэтому в каждом случае важно анализировать не только текст договора, но и фактическое содержание отношений: кто именно создавал результат, как он передавался заказчику, кто и в каком порядке вносил изменения в репозиторий, кто выполнял финальную интеграцию в мастер-версию и можно ли считать этого участника автором.

- **Пропуск «звена» в цепочке**

  Идентифицировать всех участников разработки и «собрать» всю цепочку прав бывает непросто даже при внимательном отношении. Далеко не у всех внештатных разработчиков есть доступ к внутренним системам заказчика. Репозиторий может не содержать логов, указывающих на стороннего разработчика. Если договор с ним отсутствует или не был предоставлен компанией, то существует риск «пропустить» такого разработчика или отчуждателя прав в цепочке.

- **Использование агентских компаний**

  Если в разработке использовались посреднические конструкции, это создает отдельный блок рисков. В этом случае восстановить последовательность переходов прав намного сложнее — часто ограничиваются проверкой перехода права только от посредника. Однако необходимо убедиться, что к нему изначально перешли права от привлеченных им авторов.



Илья Булгаков

советник

DÉNUO

Сейчас нередко компании привлекают удаленных сотрудников в зарубежных юрисдикциях (и их число может быть значительно). Из-за ограничений в международных расчетах для оплаты работы таких сотрудников привлекают специальные платформы или компании-прослойки, которые организуют платежи либо полностью выступают стороной в отношениях с удаленными разработчиками. Зачастую структура отношений предполагает, что права на соответствующие разработки приобретает такая компания-посредник, а вот передача прав таргету может быть либо дефектной, либо осуществляться с существенной задержкой.

- **Ошибки в определении момента перехода исключительного права**

  В договоре заказной разработки ПО следует проверить, что стороны не согласовали условие о принадлежности результата исполнителю. Также важным является наличие каких-либо гарантий исполнителя в отношении титула на созданное ПО. Если исполнитель — юридическое лицо, разработку могли осуществлять его работники или подрядчики. Если он не готов предоставить гарантии, — это повод усомниться в наличии у него титула на ПО, созданное его работниками или подрядчиками, который должен был перейти к заказчику. Неверно считать, что «режим служебности» не имеет значения в рамках отношений заказной разработки, так как права автоматически переходят заказчику. Изначально права все равно должны «появиться» у исполнителя на общих основаниях.

  В договоре авторского заказа следует проверить условие о распределении прав на создаваемое ПО. По умолчанию титул сохраняется за автором-исполнителем.

  Особенно важен анализ титула на продукт, создаваемый в рамках т. н. совместной разработки, например с партнером по СП. Такие договоры могут содержать сложные правила, регулирующие процесс создания продуктов и распределения прав в их отношении. Часто используются конструкции т. н. «предшествующих ОИС» (background IP) и «последующих ОИС» (foreground IP), принадлежащих обеим сторонам или одной их них. Такие договоры могут предусматривать ограничение на распоряжение совместно созданным продуктом, если он является производным от оригинального объекта, принадлежащего одной из сторон. Важно установить, как именно определялась принадлежность прав на созданные компоненты, какие результаты относились к исходным наработкам, а какие к новым разработкам, и как это соотносилось с фактическим вкладом сторон.

  Во всех случаях следует проверять, как определен момент перехода к компании исключительного права, и к каким обстоятельствам он «привязан».

3.2.4 Вопросы импортозамещения

В ходе юридической проверки программных продуктов довольно часто возникают вопросы, связанные с соблюдением приобретаемой компанией требований импортозамещения. Это особенно важно в случаях, когда основные заказчики компании или приобретателя относятся к публичному сектору, компания внедряет решения на объектах КИИ, участвует в государственных закупках на поставку своих решений для целей государственных нужд или планирует выйти в сегмент B2G, а также использует IT-льготы или имеет такое намерение.

В ходе исследования мы попросили экспертов прокомментировать, каким образом они проверять вопросы импортозамещения при проведении due diligence в рамках сделок с технологическими бизнесами.

#ВОПРОСЫ_ИМПОРТОЗАМЕЩЕНИЯ



Дарья Носова

партнер и руководитель практики цифрового права и интеллектуальной собственности

O_2 консалтинг

В первую очередь представляется целесообразным проверить наличие ПО в соответствующем реестре Минцифры. Если соответствующее ПО уже включено в реестр, этого, как правило, достаточно, поскольку в рамках процедуры регистрации Минцифры проводит комплексную и детальную проверку соответствия всем критериям, установленным Постановлением Правительства РФ № 1236.

В случае если ПО в реестре отсутствует и рассматривается в качестве кандидата для включения, возникает необходимость самостоятельной предварительной оценки рисков отказа в регистрации. В рамках такой оценки юридическая команда может провести базовую проверку соответствия ключевым требованиям, предъявляемым к отечественному ПО. При этом следует учитывать, что юридическая проверка не подменяет собой техническую экспертизу, а формирование однозначного вывода о соблюдении критериев возможно исключительно при тесном взаимодействии с техническими специалистами.

Как правило, указанная проверка охватывает анализ структуры правообладателя и бенефициарного владения с точки зрения преобладания российской стороны и отсутствия иностранного контроля, а также проверку титула на ПО, включая договоры с разработчиками, условия отчуждения исключительных прав и правомерность использования сторонних компонентов. Отдельное внимание уделяется анализу применяемых open source лицензий и соблюдению их условий, а также оценке правомерности ввода ПО в гражданский оборот и отсутствию договорных либо лицензионных ограничений на его распространение и использование на территории Российской Федерации. Дополнительно анализируется структура доходов от коммерциализации ПО и объем выплат иностранным лицам, связанным с его разработкой, модификацией и сопровождением.

Наряду с этим оцениваются организационные и технические аспекты, в том числе отсутствие принудительного обновления и управления из-за рубежа, преобла-

дание российской стороны в технической поддержке, доработке и модернизации ПО, а также размещение инфраструктуры хранения исходного и объектного кода, средств компиляции, активации и лицензирования на территории Российской Федерации. В рамках юридической проверки также возможно предварительно оценить наличие русскоязычного интерфейса.

В зависимости от функционального назначения ПО может потребоваться дополнительная проверка на отсутствие сведений, составляющих государственную тайну, а также наличие необходимых лицензий и сертификатов ФСТЭК и ФСБ России. Кроме того, целесообразно учитывать требования к совместимости с российскими операционными системами, включая их поэтапное введение с 2026 г.

#ВОПРОСЫ_ИМПОРТОЗАМЕЩЕНИЯ



Елена Полевая

старший юрист

KKMP LEGAL

По моему мнению, в юридическом due diligence титула на ПО наиболее сложным является проверка российского происхождения приобретаемого ПО. Подтверждение российского происхождения ПО влияет на соблюдение приобретателем требований по импортозамещению и привлечение государственного финансирования. Этот аспект приобретает особо важное значение, если у приобретателя есть критическая инфраструктура, и в нее необходимо будет интегрировать приобретаемое ПО. Это требует не только юридического анализа предоставленных документов, но также комплексного исследования всех обстоятельств, которые могут свидетельствовать о наличии у компании компетенций и возможности для разработки, развития и техподдержки ПО. На практике мы видим, что юридический due diligence этого аспекта дополняется техническим due diligence. В ходе технического due diligence устанавливается факт создания ПО приобретаемой компанией (а не переработки иностранного ПО).

Раздел 4

Техническая экспертиза в сделках Tech M&A

Преимущество или необходимость

АВТОРЫ



Анатолий Земцов
DFCenter



Роман Головацкий
DENUO

Краткие выводы

- В 2025 г. роль технической экспертизы в сделках Tech M&A возросла, в том числе при приобретении неконтролирующих долей в ИТ-активах. Основные причины: (i) повышение спроса на техническую зрелость ИТ-продуктов и их соответствие заявленным маркетинговым характеристикам; (ii) ужесточение регулирования импортозамещения; (iii) рост числа утечек данных, появление новых ИБ-угроз; (iv) активное распространение и внедрение ИИ-технологий.

- Проведение технической экспертизы целесообразно не только для выявления технических рисков продукта и инфраструктуры, но также юридических и иных рисков, наличие которых может повлиять на снижение стоимости ИТ-бизнеса, потребовать существенного изменения условий сделки или даже отказа от нее.

- Выводы технической экспертизы при приобретении ИТ-бизнесов имеют основополагающее значение для целей юридической проверки ПО и инфраструктуры, используемых приобретаемой компанией. Полученные экспертные данные позволяют правильно расставить приоритеты при проведении юридического due diligence, корректно определить периметр ключевых ИТ-активов, установить круг авторов ПО, подтвердить соответствие продукта регуляторным требованиям и сформировать план мероприятий по митигации выявленных юридических рисков.

- Существует несколько видов экспертизы, называемой в бизнес-среде «технической проверкой» ИТ-активов. К ним относятся экспертиза кодовой базы продукта, IT-инфраструктуры приобретаемой компании, методологии разработки и процессов управления жизненного цикла ПО, вопросов, связанных с ИБ.

Анализ этих блоков предполагает различные типы экспертиз, команды специалистов и используемые средства и методы исследования. Это следует учитывать при составлении технического задания на проведение такой проверки.

- Среди обстоятельств, установление которых является предметом технической экспертизы, наиболее значимыми для целей юридической проверки являются: (i) определение круга авторов ПО; (ii) декомпозиция продукта и выявление критически важных компонентов ПО; (iii) определение наиболее значимых, а также «токсичных» сторонних компонентов ПО, использованных в продукте.

Юридическая экспертиза программного продукта, лежащего в основе бизнеса ИТ-компании, направлена на то, чтобы дать правовую оценку фактическим обстоятельствам, связанным с его созданием и использованием. Между тем корректность выводов юридической экспертизы **всегда зависит от того, насколько полно и правильно установлены эти обстоятельства**. Таким образом, юридическая проверка в части вопросов титула и правового режима продукта, по сути, носит вторичный характер по отношению к технической.

Установление соответствующих фактов **возможно лишь с участием технических специалистов**, поэтому роль технической экспертизы значительна. Без ее проведения выводы, сделанные в ходе юридического анализа, могут оказаться ошибочными или нерелевантными. Так, неверное определение лиц, внесших существенный вклад в кодовую базу продукта, может привести к неправильной оценке титульных рисков. Безусловно, в рамках юридической проверки юристы также проводят самостоятельную работу по сбору информации, включая интервью и анализ документов. Однако без технической верификации такой информации правовые выводы, основанные на ней, будут носить лишь вероятностный характер.

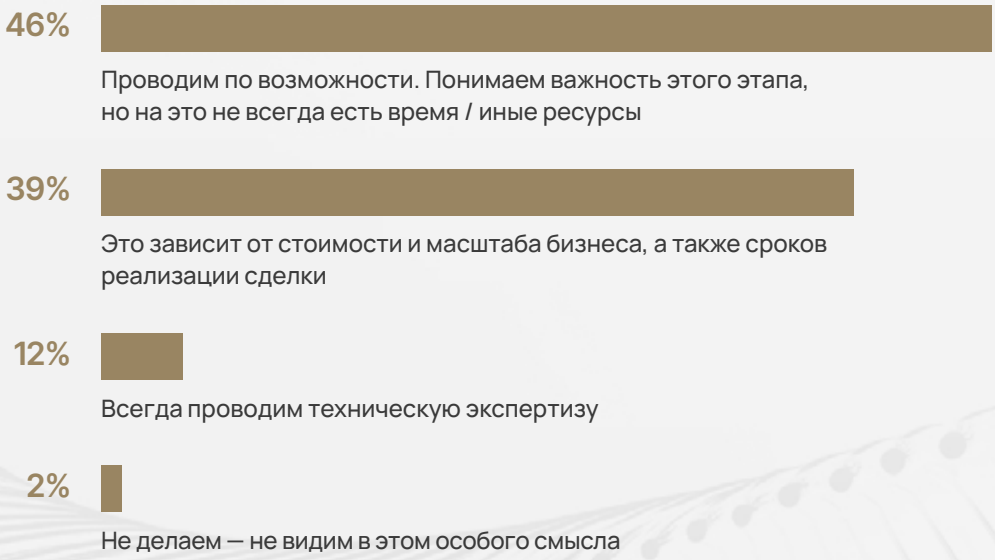
Кроме того, техническая экспертиза позволяет определить **наиболее важные части продукта и тем самым сфокусировать объем юридической проверки**. Это особенно актуально для сложных многокомпонентных систем, проверка каждого элемента которых потребует значительных временных и материальных ресурсов в условиях ограниченных сроков due diligence. Соответственно, в отсутствие технической экспертизы юридический анализ не будет в достаточной степени эффективным.

4.1 Техническая экспертиза ПО в сделках Tech M&A 2025 г.

Мы провели опрос, в рамках которого попросили участников сделок Tech M&A отметить, проводят ли они техническую экспертизу при приобретении ИТ-бизнесов.

#РЕЗУЛЬТАТЫ_ОПРОСОВ

Проводите ли вы техническую экспертизу при приобретении ИТ-бизнеса?



По данным Опроса по аспектам к Tech M&A (41 респондент).

Результаты другого опроса, проводимого в рамках этого исследования, показали, что в 2025 г. участники сделок Tech M&A стали чаще проводить техническую экспертизу при приобретении IT-компаний в целом. В том числе большее внимание стали уделять анализу **кодовой базы программных продуктов**. Также респонденты отметили усиление внимания инвесторов к анализу **ИБ-рисков, связанных с утечками и уязвимостями ИТ-контура** приобретаемой компании и самого программного продукта.

#РЕЗУЛЬТАТЫ_ОПРОСОВ



Стали чаще делать техническую экспертизу ПО при принятии инвестиционных решений в 2025 г.



Стали чаще делать техническую экспертизу при приобретении контролирующих долей в ИТ-компаниях и в сделках, предполагающих интеграцию программных продуктов

По данным Опроса по структурированию сделок Tech M&A в 2025 г.



Стали при приобретении ИТ-компаний уделять больше внимания ИБ-рискам, связанным с утечками данных и безопасностью ИТ-контура

Мы попросили участников сделок Tech M&A прокомментировать результаты опросов, в том числе отметить: (i) проводят ли они технический due diligence при принятии инвестиционных решений; (ii) влияет ли на решение о проведении такой экспертизы масштаб и стоимость бизнеса, а также размер приобретаемого пакета; (iii) используют ли они результаты технической экспертизы ПО, баз данных и других ИТ-активов при проведении их юридической проверки и для целей структурирования сделки.



Алексей Мустяца

директор, управление слияний и поглощений

СОВКОМБАНК

В 2025 г. юридический DD ПО все чаще проводился в связке с техническим аудитом, особенно при приобретении контроля или последующей интеграции технологии. Результаты tech-DD фактически становились необходимым элементом для оценки титула, состава кода и связанных рисков.



Сергей Чапаев

партнер корпоративной практики

ELWI

Исходя из нашего опыта, технический due diligence ПО в той или иной форме целесообразен в большинстве сделок по приобретению ИТ-бизнеса, обладающего значимым проприетарным ПО, за исключением, пожалуй, частных случаев приобретения мелких пакетов в стиле private equity, однако степень доскональности такой проверки может сильно варьироваться в зависимости от размера сделки и специфики целевой компании. Одним из ключевых компонентов подробной проверки является аудит исходного кода ПО, по результатам которого можно оценить как риски претензий со стороны третьих лиц (например, вследствие использования open source компонентов или элементов кода, разработанного третьими лицами в отсутствие необходимых лицензий), так и общее качество кода, что в определенных случаях может напрямую влиять на коммерческие параметры сделки. В частности, в результате проверки могут быть выявлены существенные критические уязвимости в самом коде или обнаружена принципиальная несовместимость с платформой приобретателя в силу фундаментально отличающихся подходов к архитектуре ПО, что может быть важно как с точки зрения полноценной интеграции, так и для масштабирования силами покупа-

теля. Кроме того, технический due diligence помогает выявить ситуации, при которых ПО — а следовательно, и сам таргет — имеет критические зависимости от группы продавца (например, ПО полагается на важные элементы, которые остаются за периметром сделки). В зависимости от ситуации, аудит может проводиться как силами покупателя, так и специализированными провайдерами таких услуг, что зачастую является предпочтительным для продавцов вариантом по соображениям конфиденциальности. Кроме того, хорошее понимание исходного кода ПО целевой компании может значительно облегчить интеграцию с группой покупателя в будущем, если она предполагается.



Антон Джуплин
партнер
АЛРУД

АЛРУД самостоятельно не проводит технический DD ПО, при этом наши клиенты проводят технические DD ПО в случае приобретения ИТ-бизнеса.

Юридический DD может быть полноценно проведен без результатов технического DD, поскольку в рамках юридического DD мы исходим из достаточности и достоверности информации, предоставленной таргетом. Впоследствии в договор часто включаются положения, в соответствии с которыми продавец гарантирует, что определенный список ПО (который проверялся в рамках юридического DD) является достаточным для ведения бизнеса таргета.

Вместе с тем наличие результатов технического DD полезно для того, чтобы удостовериться в корректности предоставленной таргетом информации. Это позволяет исключить ошибки локальных исполнителей, которые, как правило, являются юристами и не всегда могут корректно понять вопросы, если они связаны с техническими аспектами (например, юристы могут не иметь достаточной картины о зависимости ПО таргета от другого ПО).



Денис Борисов

советник корпоративной практики

NEXTONS



Ксения Михайлова

советник корпоративной практики

NEXTONS

В нашей практике клиенты в большинстве случаев инициируют технический due diligence ПО. При этом проверка осуществляется не только при приобретении контрольного пакета, но и при приобретении существенной миноритарной доли. Среди основных причин проведения технического due diligence можно выделить: (а) намерение инвестора развивать продукт, а не только получить финансовый результат; (б) необходимость оценки технических рисков, способных повлиять на стоимость или реализацию сделки.

Помимо стремления лучше узнать актив, точнее его оценить и корректнее его интегрировать в свой бизнес, приобретатель также учитывает текущую судебную практику, которая придерживается «принципа caveat emptor». Иными словами, приобретатель стремится минимизировать правовые риски, которые непосредственно связаны с технологической основой актива и в ряде случаев могут быть выявлены только на техническом уровне.



Софья Смирнова

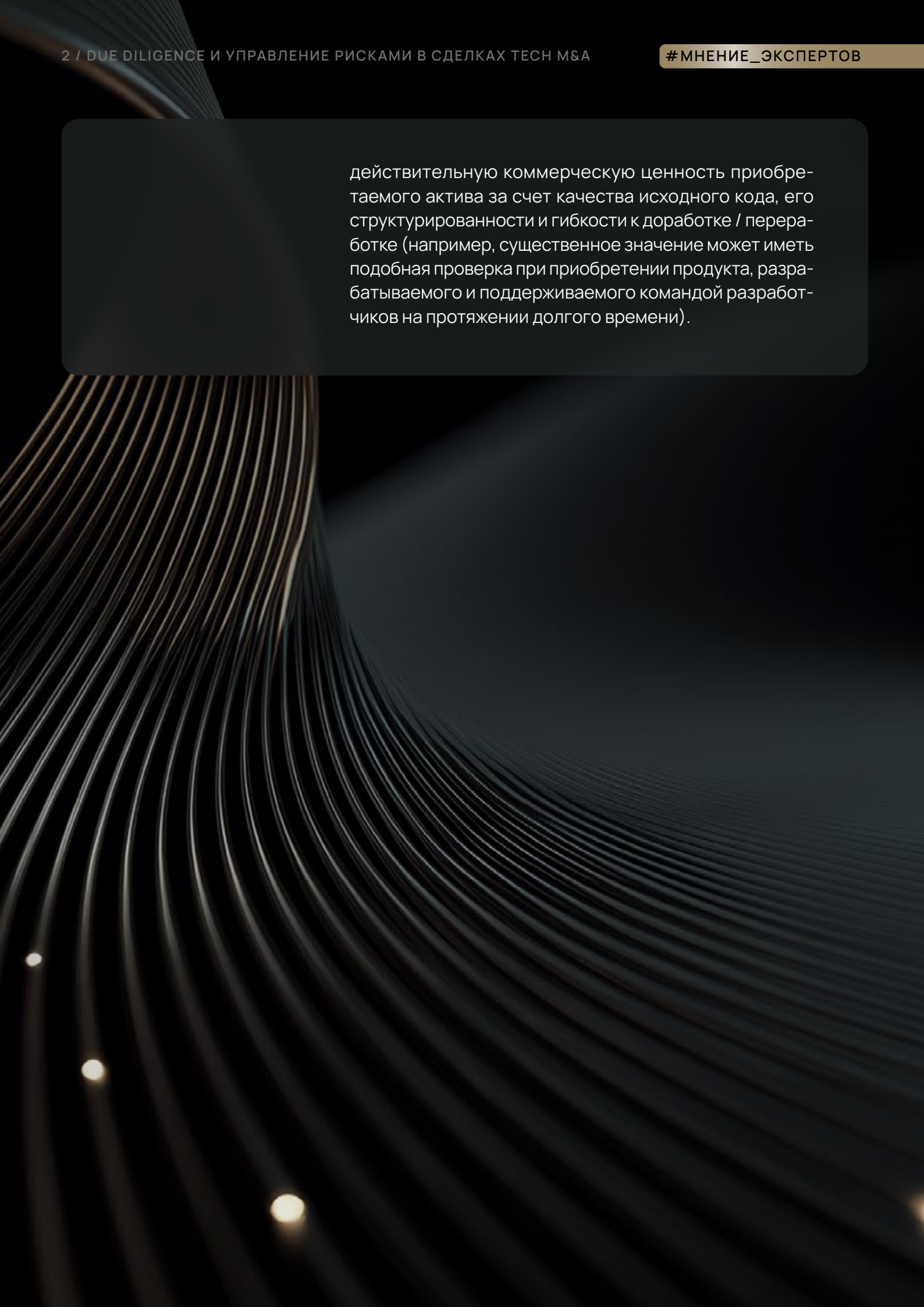
советник M&A и корпоративной практики

O2 консалтинг

Технический due diligence представляется для Tech M&A крайне важным этапом проверки, без которого юридическая проверка станет неполной или будет недостаточно глубокой. В процедуру проверки, как правило, входит изучение репозитория на предмет наличия «токсичных» опенсорсных компонентов и установления списка авторов. Данные вопросы имеют прямое отношение к возможным юридическим выводам.

Вместе с тем технический due diligence имеет и свои задачи — например, помочь покупателю установить

действительную коммерческую ценность приобретаемого актива за счет качества исходного кода, его структурированности и гибкости к доработке / переработке (например, существенное значение может иметь подобная проверка при приобретении продукта, разрабатываемого и поддерживаемого командой разработчиков на протяжении долгого времени).



Участники сделок Tech M&A отмечают, что технический due diligence позволяет выявить ряд проблемных вопросов, которые могут не упоминаться в коммуникациях с командой приобретателя и презентационных материалах продукта. В инвестиционной среде в 2025 г. более явно начал формироваться запрос на проведение технических проверок приобретаемого актива. Такой тренд отмечается не только в сделках по приобретению контроля, в том числе в целях интеграции продукта в собственный ИТ-контур, но и при инвестировании в менее крупные доли в активе, в том числе в качестве финансового инвестора.

Предпосылки роста интереса инвесторов к технической проверке

Многие эксперты, опрошенные нами в ходе проведения исследования, отметили несколько причин возросшего в 2025 г. спроса на прединвестиционную проверку технической зрелости продукта и его соответствия заявленным характеристикам. Среди ключевых причин участники рынка выделяют следующие:

- **Ужесточение требований к импортозамещению**

  Среди таких требований в том числе запрет на допуск к государственным и муниципальным закупкам и интеграции на объектах КИИ ПО, которое не включено в государственные реестры.

- **Рост числа утечек данных**,

  в том числе в «чувствительных» сегментах, появление новых типов ИБ-угроз и рисков.

- **Повсеместное распространение ИИ**

  В сделках с ИИ-активами, как и при их внедрении для собственных нужд, в том числе для целей ИИ-трансформации, предварительная техническая экспертиза становится ключевым этапом.

- **Рост интереса инвесторов к реальному качеству активов**

  Все больше инвесторов проявляют интерес к проверке соответствия действительности заявленных характеристик продукта и его технической состоятельности, в том числе способности продукта выполнять тот функционал, который описан в маркетинговых материалах, и возможности его развития и масштабирования в соответствии со стратегическими планами приобретателя или инвестора.

4.2 Типы и объем технической экспертизы



Илья Булгаков
советник
DÉNUO

Обычно техническая проверка (technical due diligence) фокусируется на организационных аспектах разработки (наличии технического долга, покрытии кода тестами, наличии опенсорсных решений, использовании лучших практик и т. д.), а также потенциальной масштабируемости решения и постпродажной интеграции, а не на детальном анализе самого кода. Иногда техническая проверка (technical due diligence) сопряжена с проверкой на кибербезопасность, где акцент делается на защищенности систем и их устойчивости к кибератакам.

Исходя из нашей практики, непосредственно сам код детально и подробно анализируют, когда покупатель или инвестор в силу своих внутренних причин инициирует подробный аудит исходного кода, а также когда продукт представляет собой уникальное решение на рынке с сильной технической составляющей.

Объем технической экспертизы зависит **от типа и специфики продукта, решаемых им задач, а также планов приобретателя или инвестора в отношении развития компании**. В бизнес-среде термин «техническая экспертиза» для целей M&A зачастую употребляется в широком смысле. В зависимости от специфики продукта она может включать различные блоки проверки, а также относиться к различным уровням анализа — продуктовому или инфраструктурному.

#УРОВНИ_ТЕХНИЧЕСКОЙ_ЭКСПЕРТИЗЫ

По мнению технических экспертов, принимающих участие в исследовании, по критерию относимости к продукту или инфраструктуре можно выделить следующие вопросы технического анализа:

Вопросы технической экспертизы на уровне продукта

- Реальность продукта и его соответствие заявленным характеристикам.
- Качество и содержание кода продукта.
- Наличие и объем open source компонентов, наличие среди них «ограниченных» в использовании элементов.
- Наличие в продукте фрагментов проприетарного кода третьих лиц, ИИ-сгенерированного кода.
- История создания продукта, участники разработки (потенциальные авторы).
- Уровень ИБ-угроз на уровне кода.
- Масштабируемость, включая вопросы достаточности инфраструктуры.
- Объем технического долга.

Вопросы технической экспертизы на уровне инфраструктуры компании

- Отказоустойчивость, включая достаточность защиты от DDoS-атак.
- ИБ-защита ИТ-контура, надежность межсетевых экранов и т. п.
- Совместимость технологических стеков приобретаемого бизнеса и покупателя.
- Соответствие реальных технических возможностей компании обязательствам, декларированным перед клиентами в SLA.

Вопросы ИБ, которые являются крайне важными для оценки рисков определенной категории продуктов, по мнению ряда экспертов, не относятся к задачам, решаемым в рамках классической технической экспертизы, а являются предметом отдельного типа проверки. Однако такое деление весьма условно. При подготовке общего задания на анализ технических и ИБ-вопросов целесообразно получить запрос не только представителей технической команды, но ИБ-специалистов, а также инхаус-юристов, которые будут непосредственно анализировать юридические IT / IP-вопросы продукта (своими силами или с привлечением внешних консультантов).

#БЛОКИ_ТЕХНИЧЕСКОГО_АУДИТА

В объем задания на проведение технической (в широком смысле слова, включая вопросы ИБ) экспертизы сервиса на основе B2B или B2C платформы могут входить следующие вопросы:

- **Техническая реализация платформы**: архитектурные требования и принципы, анализ функциональных модулей (ядро, продуктовые сервисы), технологический стек, возможность масштабирования, автономность продукта от работы внешних сервисов, процессы логирования, форматы взаимодействия с внешним контуром.
- **Характеристики функционирования системы**: число уникальных записей, число запросов в день, среднее время ожидания ответа, в т. ч. при пиковой загрузке, общая доступность сервиса в разрезе различных уровней нагрузки.
- **Кодовая база**: языки программирования и фреймворки, используемые для fullstack-разработки продукта, лицензии, по которым они распространяются, процессы тестирования, журналирования, мониторинга, поддержки кодовой базы, наличие уязвимостей на уровне кода.
- **Анализ репозиториев, круг авторов и объем их вклада**: лица, которым был предоставлен доступ в репозиторий разработки, их роли, данные идентификации и аутентификации, % кода, созданного каждым из них, в том числе от общего числа коммитов и общего числа строк кода, ранжирование авторов по наиболее критичному вкладу с точки зрения объема и значения в рамках всего продукта.
- **ИТ-инфраструктура (программная и аппаратная)**: среды развертывания, в том числе продакшен, разработка и тестирование, включая применительно к каждой среде (если применимо) — инструментарий управления различными задачами и изменениями в кодовой базе, вопросы идентификации, аутентификации и авторизации запросов, средства обеспечения отказоустойчивости сервисов, доступности баз данных, используемые ЦОДы, сегменты сетей, используемое сетевое оборудование, требования по доступности сервисов, политика реагирования на инциденты.
- **Управление жизненным циклом разработки ПО**: методология разработки ПО, процессы обновлений и релизов, принципы версионирования, разграничение доступов к «мастер-ветке», вопросы организации тестирования, отладки, рефакторинга, технической поддержки.
- **ИБ-вопросы**: предоставление и безопасность доступов, средства защиты от таргетированных атак, антивирусная и внутрисетевая защита, реагирование на ИБ-инциденты.

4.3 Взаимосвязь технической экспертизы и юридической проверки

Помимо **стандартного** объема технической проверки, существует множество вопросов, **которые имеют важное, а порой — критическое значение для целей точности проведения юридической проверки** ПО, данных и инфраструктуры. Наличие предварительных выводов по этим вопросам, подготовленных техническими экспертами, является прекрасным подспорьем при анализе юридических IP / IT-аспектов деятельности приобретаемой компании.

В частности, **технический due diligence позволяет выявить следующие обстоятельства**, имеющие важное значение для правильной юридической квалификации и разрешения соответствующих вопросов (приведены далее в разрезе основных этапов работы по сделке):

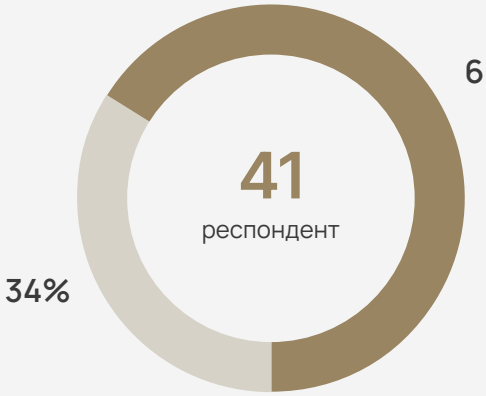
Юридическая проверка

1. Определение **архитектуры** продукта приобретаемой компании (например, модульно-монолитная или микросервисная) и сред его развертывания, определение общего количества модулей, подсистем и классов в рамках единого продукта, выделение наиболее значимых из них по заданным критериям (выручка, затраты и скорость замены или «переписывания» компонентов ПО, вклад авторов в их разработку), наличие у ПО признаков производного или составного произведения, в том числе определение периметра ключевых систем и модулей, без которых невозможно нормальное функционирование продукта, отсутствие которых приведет к простою бизнеса, потребует дорогостоящей замены соответствующих компонентов.

   Это позволит правильно организовать и приоритизировать юридическую проверку, декомпозировать программный продукт на различные типы элементов, определить применимые правовые режимы к совокупности ИТ-активов.

2. Установление **круга авторов ПО**, степени их вклада в разработку и поддержание продукта. Это позволит существенно повысить точность выводов юридической проверки в отношении титульных рисков и установления цепочки переходов прав на продукт, а в некоторых случаях — избежать серьезных ошибок при анализе этих вопросов.

#РЕЗУЛЬТАТЫ_ОПРОСОВ



Полностью делегируют технической команде вопрос установления круга авторов ПО, так как считают, что юристы не могут достоверно определить авторов

По данным Опроса по аспектам Tech M&A.

3. Выявление круга **ключевых разработчиков ПО**, от которых существенно зависит разработка, поддержание и развитие продукта, увольнение или прекращение работы с которыми после закрытия сделки могут существенно снизить эффективность функционирования продукта. Для юристов это послужит обоснованием более тщательного анализа правоотношений с указанными разработчиками, в том числе вопросов их мотивации и мероприятий юридического характера, направленных на их удержание в компании.

4. Определение фрагментов продукта, **созданных с помощью инструментария ИИ**, например, в рамках применения технологии вайб-кодинга, а также степени значимости таких компонентов для продукта в целом и связанных с ними рисков. Если речь будет идти о важных для продукта **компонентах**, фокус юридического анализа необходимо направить на оценку охраноспособности таких фрагментов, а в случае их **соответствия** критериям охраноспособности — на установление авторства в их отношении.

5. Определение **количества самостоятельных информационных элементов** в рамках используемых крупных массивов данных, установление наличия в датасетах персональных данных, а также применение методов автоматизированного сбора (парсинга) при формировании таких массивов данных. Это позволит юристам оценить наличие презумпции существенности затрат, связанных с созданием соответствующих датасетов, и сделать вывод о наличии титула (смежного права). Также это даст возможность оценить прочие риски, связанные с обработкой ПДн, и риски нарушения прав третьих лиц при использовании таких данных в рамках продукта. Эти вопросы особенно актуальны для решений, использующих ИИ-технологии.

Подготовка ИТ-активов к продаже и реструктуризация

6. **Оценка соответствия ПО требованиям к российскому или евразийскому ПО**. В частности, это может быть актуально для компаний: (i) которые планируют подать заявку на включение в государственные реестры (РРПО или ЕРПР[18]), в том числе в целях использования налоговых льгот, участия в закупках на поставку ПО для государственных нужд или интеграции с объектами КИИ; (ii) ПО которых уже было включено в указанные реестры и которые уже используют соответствующие льготы и преимущества. Позиция регулятора по поводу повторных проверок ПО, уже включенного в реестры, еще формируется. Однако если список «запрещенных компонентов» будет расширяться, вероятность повторных проверок повышается.

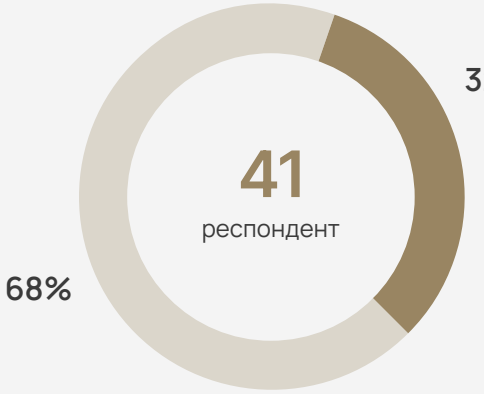
   Эти данные технической проверки позволят юристам корректно сформировать «дорожную карту» мероприятий, связанных с процессом включения ПО в соответствующие реестры, а также обозначить риски, связанные с возможным исключением ПО из реестра, например, по решению суда.

> **Юристы не могут установить авторство ПО с существенной степенью достоверности. Они могут лишь предположить наличие авторства, используя критерии охраноспособности. Однако такие выводы без валидации техническим экспертом будут носить исключительно вероятностный характер и не могут быть оценены как достоверные.**

7. Определение количества **open source компонентов**, юрисдикции их происхождения, характера лицензий, по которым они распространяются, возможности их оперативной замены и наличия отечественных аналогов, требований раскрытия кода всего продукта, возможности митигации рисков путем их динамического линкования, совместимости с другими компонентами в рамках продукта. Это позволит юристам проанализировать наиболее «токсичные» лицензии и, в случае высоких рисков, адресовать вопросы бизнес-команде, в том числе о замене соответствующих компонентов до закрытия сделки или в ближайшее время после него. Также это позволит оценить юридические риски утечки данных (в том числе персональных), связанных с использованием зарубежных репозиториев, сред разработки и управления задачами, а также санкционные риски.

[18] Реестр евразийского программного обеспечения (Единый реестр программ для электронных вычислительных машин и баз данных из государств-членов Евразийского экономического союза, за исключением Российской Федерации).

#РЕЗУЛЬТАТЫ_ОПРОСОВ



Считают вопросы правомерности использования open source ПО в составе продукта приоритетными в рамках due diligence ПО

По данным Опроса по аспектам Tech M&A.

8. Содействие юридической команде в реализации **мероприятий по митигации рисков** ПО, в т. ч. титульных: (i) определение критически значимых компонентов, в отношении которых риски следует урегулировать до закрытия сделки; (ii) восстановление документооборота в отношении прав на ПО, в частности корректное описание отдельных частей ПО и задач по их разработке, определение авторов компонентов, в отношении которых были выявлены риски, а также периода создания такого компонента и т. п.; (iii) определение перечня менее критичных элементов, устранение рисков в отношении которых может быть перенесено на более поздний этап, в том числе после закрытия сделки; (iv) определение компонентов, которые необходимо юридически и физически перевести в контур компании до закрытия сделки.
9. Использование в рамках продукта методов и технических средств (например, криптографии), которые требуют сертификации регуляторов (ФСТЭК, ФСБ) или получения соответствующей лицензии. Юристы не могут самостоятельно оценить такие риски. При этом отсутствие разрешительной документации может вызвать негативные юридические последствия.

Структурирование сделки

10. Помощь юридической команде по **отдельным вопросам структурирования сделки**, в частности: (i) корректное **описание продукта** и его систем в составе ИТ-контура приобретаемой компании, включая составление точного перечня всех ключевых систем и модулей продукта, open source и проприетарных сторонних компонентов, предоставление ссылок на соответствующие репозитории, их хеш и т. п.; (ii) оценка адекватности **формулировок заверений** и потерь, если они связаны с техническими аспектами; (iii) определение **размера имущественных потерь** при утрате критичных компонентов ПО; (iv) определение **перечня действий**, которые компания должна и не должна совершать в отношении ИТ-активов и инфраструктуры в период с подписания сделки до ее закрытия (pre-closing obligations) и после закрытия сделки (post-closing obligations); (v) описание «технических» КПЭ и триггеров и способов их верификации для целей опционов, механики earn-out, условий возмещения потерь и т. п.

11. Определение **стоимости замещения спорных ключевых компонентов ПО**, как в денежном выражении, так и в человеко-часах, «переписывания» такого фрагмента внутренними силами команды после сделки, количества и ролей специалистов, которые могут понадобиться для этих целей. Это позволит юристам и финансистам учесть эти вопросы при разработке системы защиты от титульных или иных рисков, связанных с ПО, материализация которых может привести к юридической или физической невозможности использовать такие фрагменты ПО. Также это даст возможность оценить стоимость одного дня простоя бизнеса или продукта, индикативный размер убытков, в том числе при использовании концепта «заранее оцененных убытков» и т. п.

Интеграция

12. Определение ИТ-контура приобретаемой компании и сред развертывания продукта, **целостности кодовой базы, возможности ее консолидации, если компания не контролирует все компоненты ПО и зависима от третьих лиц**, возможности миграции кодовой базы продукта и всех артефактов в контур приобретателя (если это необходимо по условиям сделки), сроков и условий реализации такой миграции. Это позволит юристам более точно определить основные мероприятия и сроки их проведения, связанные с процессом интеграции продукта, а также более корректно описать связанные с ними правовые последствия.

4.4 Управление рисками при проведении технической экспертизы

#РИСКИ_РАСКРЫТИЯ_КОДА

Одним из важных вопросов при проведении технической экспертизы является обеспечение защиты раскрываемых объектов проверки — кодовой базы и инфраструктуры. Этот аспект имеет большое значение для компании, являющейся объектом сделки, которая управляет продуктом и средами его разработки и поддержки. Проведение технической экспертизы обычно осуществляется на ранних этапах сделки, когда компания и ее владельцы не имеют полной уверенности в том, что сделка состоится и что ее условия окажутся приемлемыми. На момент предоставления команде инвестора или его консультантам доступа к информационным системам и репозиториям компания и ее собственники еще могут быть не связаны никакими обязательствами, имеющими юридическую силу, и зачастую такая экспертиза проводится на основании рамочных или «понятийных» договоренностей.

Для компании такая ситуация может повлечь риски утечек кодовой базы и привести к утрате конкурентных преимуществ в случае отказа приобретателя от сделки, в т. ч. мотивированного наличием в коде каких-либо существенных дефектов, обнаруженных при проверке. Иными словами, компании, действуя «на доверии», небезосновательно опасаются недобросовестных практик и в ряде случаев могут поставить вопрос о применении средств защиты против таких рисков.

Мы попросили технических экспертов и юридических M&A-консультантов, сопровождающих сделки с технологическими активами, поделиться опытом урегулирования таких вопросов в различных ситуациях на примере собственной практики.

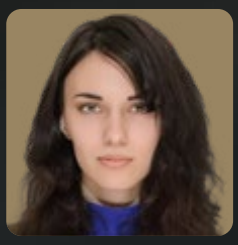


Илья Булгаков

советник

DÉNUO

В нашей практике встречались случаи, когда контрагенту по сделке раскрывался практически весь исходный код перед сделкой. В этом случае заключалось соглашение о неразглашении (NDA), однако в других документах по сделке, включая основные условия сделки (term sheet), положений, касающихся раскрытия кода и ответственности получающей стороны, как правило, не предусматривалось.



Анастасия Нерчинская

Включать ли в term sheet и, тем более, транзакционную документацию какие-либо положения, обеспечивающие защиту продавца и его ИТ-активов от выхода покупателя из переговоров по мотивам дефектов кодовой базы, выявленных в рамках due diligence, — во многом зависит от силы переговорной позиции сторон сделки.

В моей, довольно обширной, практике сопровождения сделок Tech M&A, как в консалтинге, так и на стороне in-house бизнес-команды, мне ни разу не встречались ситуации, когда бы приобретаемая компания или продавец поднимали вопрос о включении в документы по сделке или даже в необязывающую документацию каких-либо положений, защищающих их на случай отказа покупателя или инвестора от сделки в случае обнаружения проблем с кодом или иных неудовлетворительных результатов технического due diligence. При том, что техническая проверка практически всегда проводилась в том или ином объеме, код и доступы к информационным системам приобретаемой компании раскрывались на основе кросс-NDA, заключаемых между компанией и покупателем (что на моей практике встречалось гораздо чаще), либо компанией и внеш-

ним техническим экспертом, в том числе привлеченным покупателем, если проверку проводила сторонняя организация. В том числе когда сделка совершалась на принципах конкурентного M&A-процесса. В NDA при этом может включаться список лиц, которым были предоставлены доступы к системам, у каждого из которых можно запросить персональное обязательство о неразглашении.

В случае приобретения IT-компании стратегическим покупателем, особенно если он выплачивает премию к цене, сложно представить ситуацию, чтобы он согласился на включение каких-то обязывающих положений, связанных с его правом на предварительный аудит кода и фактического состояния продукта. При этом он может согласиться на требования покупателя использовать различные средства технологической защиты при проведении технической проверки, начиная от запрета на выгрузку кода и сегментирования доступа по критерию важности ПО, заканчивая проведением проверки «на территории и под контролем продавца / компании» с видеофиксацией процесса.

При этом довольно распространена ситуация, когда на уровне term sheet стороны сделки согласовывают проведение различных проверок приобретаемой компании, в том числе технической, если речь идет о покупке ИТ-бизнеса. В этом случае может добавляться оговорка о том, что по итогам проверок может быть скорректирована цена, перечень отлагательных условий закрытия сделки или необходимость пересмотра структуры сделки, а также — право покупателя отказаться от сделки, если он посчитает неудовлетворительными результаты проверки. Но мне не встречались случаи, когда право на отказ покупателя от сделки требовало бы обоснования именно в связи с фактом раскрытия кода и получения покупателем доступа к информационным системам компании, сохранением у команды покупателя «остаточных знаний», объективации материальности выявленных дефектов.

Это, вероятно, связано с распространенной позицией о том, что риски кодовой базы в большинстве случаев не считаются принципиально неустранимыми и «безнадежными» даже в запущенных случаях, в том числе в компаниях с высоким уровнем технического долга. Если речь о том, что в компании могут быть серьезные проблемы с ПО или инфраструктурой — на этапе подписания необязывающих документов по сделке стороны «держат в голове» такие средства их митигации, как «переписывание» фрагментов кода или корректировка условий сделки. Есть немалая вероятность, что TS будет очень долго согласовываться, и сделка может сорваться уже на этом этапе, если продающая сторона будет настаивать на особой «защите» против раскрытия кода для целей технического аудита, помимо стандартного NDA.

Представляется, что в российской практике подход, требующий обеспечения защиты интересов компаний от утечек на случай срыва сделки, не является широко распространенным. Однако в сделках с участием иностранных компаний на стороне продавца такие ситуации, возможно, более распространены. В целом такой подход в некоторых ситуациях представляется разумным, но опять же все зависит от конкретных обстоятельств сделки.



Анатолий Земцов

управляющий партнер

dfcenter

В практике нашей компании, а также в известной нам практике коллег предоставление «объектов исследования» или доступ специалистов в ИТ-контур продаваемой компании осуществляется исключительно с заключением NDA, иногда трехсторонним (продавец, покупатель, провайдер Tech DD).

В тех случаях, когда в компании-таргете введен и функционирует режим коммерческой тайны (98-ФЗ[19]), по требованию заказчика проведения исследования процедура может быть дополнена подписанием необходимых обязательств о неразглашении информации, составляющей коммерческую тайну, передачей объектов и доступов под акт. Причем подписание может быть затребовано и у провайдера как организации, и персонально у специалистов-участников проектной команды как физических лиц (что представляется избыточным).

Отдельно можно выделить еще один уровень конфиденциальности — в случае продажи компании (доли в компании), разрабатывающей ИТ-решения для государственных нужд, особенно в сфере ИБ и ГОЗ[20]. Тут потенциально могут возникнуть вопросы не только коммерческой, но и государственной тайны. Наличие таких объектов в контуре Tech DD подразумевают необходимость наличия у провайдера соответствующих допусков и лицензии.

Касательно вопросов обеспечения информационной безопасности — в договоре на оказание услуг Tech DD зачастую прямо указываются обязательства провайдера по обеспечению определенного уровня ИБ внутри уже своего контура.

[19] Федеральный закон № 98-ФЗ «О коммерческой тайне» от 29.07.2004 г.

[20] Государственный оборонный заказ.



Сергей Колобов

советник

NIKOLSKAYA consulting

Среди особенностей процедуры due diligence применительно к сделкам Tech M&A можно выделить:

- проведение аудита кода / технического аудита параллельно с юридической проверкой, результаты которого напрямую влияют на состав заверений и оснований для возмещения потерь, включаемых в документацию;
- тщательную проверку авторства ПО и баз данных, где особый фокус направлен на проверку трудовых договоров с сотрудниками таргета на предмет содержания в них положений о принадлежности результатов их работ работодателю;
- определение сторонами ключевого ПО и продуктов, в отношении которых осуществляется углубленная проверка титула.

Еще одной особенностью due diligence в рамках сделок Tech M&A является его формализация в рамках обязывающей документации, что несвойственно сделкам M&A, где процедура due diligence проводится на этапе подготовки обязывающей документации, но до ее подписания. В сделках Tech M&A продавец заинтересован, чтобы аудит кода его продуктов или раскрытие информации о ноу-хау корреспондировали обязательству покупателя приобрести актив. Такой подход требует ответа на следующие вопросы в документации: как описать положительные и отрицательные результаты due diligence, как урегулировать споры в рамках предоставления информации продавцом покупателю, при каких обстоятельствах покупатель вправе отказаться от сделки, какой будет ответственность покупателя за необоснованный отказ и т. д. Все эти особенности важно учитывать уже при составлении меморандума о намерениях между сторонами.



Булат Жамбалнимбуев

партнер и руководитель корпоративной практики

NEXTONS



Денис Борисов

советник корпоративной практики

NEXTONS

Все сделки Tech M&A, в сопровождении которых мы участвовали в 2025 г., так или иначе предусматривали проведение предпродажной реструктуризации приобретаемого (отчуждаемого) актива.

Помимо стандартных вопросов структурирования сделки для устранения или минимизации выявленных рисков, оптимизации налогов и долговой нагрузки таргета, стороны фокусируются на необходимости обеспечения: (i) бесшовной миграции ключевого IP, ПО (кода), данных, команды и контрактов на чистую холдинговую (субхолдинговую) структуру без ущерба для бизнес-периметра продавца и в зависимости от запроса покупателя, (ii) дальнейшей интеграции соответствующих активов в контур покупателя.

В свою очередь, для того чтобы разработать адекватную дорожную карту предпродажной реструктуризации, требуется высокая степень вовлеченности продавца и глубокий уровень погружения в особенности функционирования приобретаемых активов со стороны покупателя. Это обусловливает необходимость проведения скрупулезного комплексного анализа структуры владения и оценки (в т. ч. технической) активов (IP, ПО, данные) для выявления существующих проблемных аспектов и выработки решений по оптимизации структуры владения, централизации прав на результаты интеллектуальной деятельности с устранением «размытых» цепочек авторства и владения и т. п.

С практической точки зрения, в этом и заключается одна из ключевых сложностей сделок Tech M&A:

1. С одной стороны, проведение такого анализа необходимо для того, чтобы выявить особенности функционирования бизнеса (прежде всего, в части IT-инфраструктуры и зависимости от внешних сервисов и подрядчиков, использования открытого кода и т. п.) и предотвратить возникновение непредвиденных затрат на миграцию и рисков отключения сервисов;

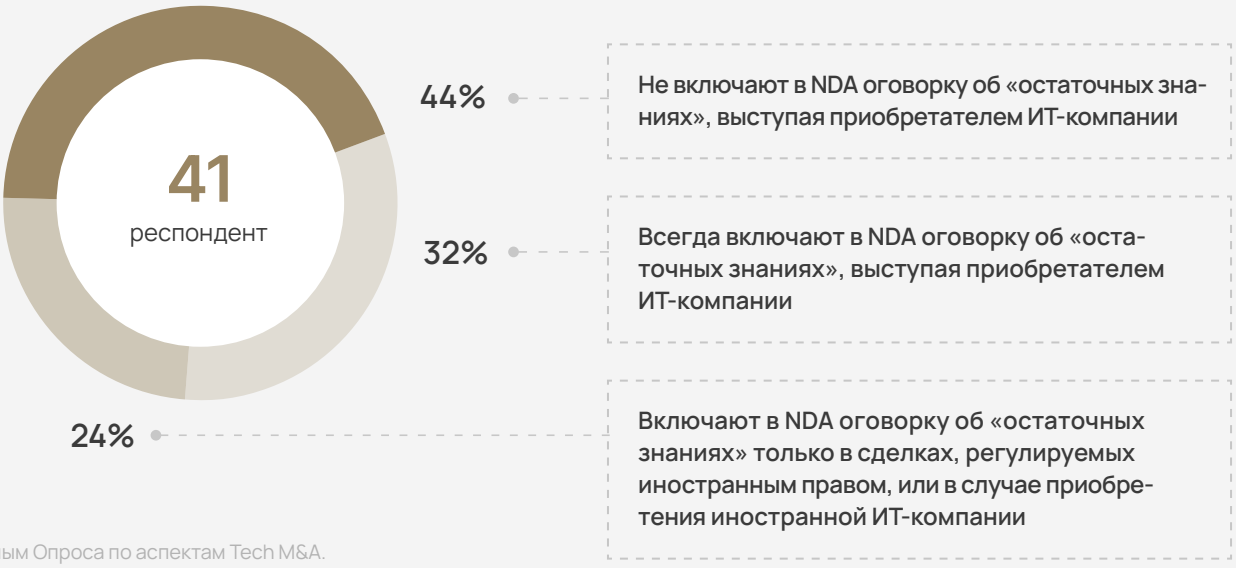
2. С другой стороны, предпродажная реструктуризация глубоко интегрированного продукта / сервиса / решения занимает длительное время и может повлечь обесценивание актива через утечку ключевых членов команды (особенно в высокотехнологичных компаниях с уникальной экспертизой, где существует очевидная зависимость от экспертизы разработчиков — не основателей).

#ОГОВОРКА_ОБ_ОСТАТОЧНЫХ_ЗНАНИЯХ

Проведение технического due diligence связано с еще одним важным вопросом, который касается т. н. «остаточных знаний» команды приобретателя или привлеченных им технических консультантов до подписания транзакционной документации.

#РЕЗУЛЬТАТЫ_ОПРОСОВ

Использование оговорки об остаточных знаниях при проведении технического аудита ПО



По данным Опроса по аспектам Tech M&A.

Несмотря на «экзотичность» и чужеродность для российского правопорядка оговорки об «остаточных знаниях», результаты опроса, которые оказались довольно поляризованными, показывают значительную популярность такого инструмента. Существенная часть респондентов (**68%**), выступая на стороне приобретателя, использует условие об «остаточных знаниях» на случай срыва сделки, чтобы защитить свою команду от претензий продавца. При этом **44% респондентов** всегда использует такую оговорку, а **24%** — лишь в Tech M&A сделках с иностранным элементом.

Оговорка об «остаточных знаниях» призвана защитить потенциального покупателя технологического актива от возможных требований продавца или компании, сделка в отношении которой не состоялась, но команда покупателя ранее получила доступ к ИТ-системам и кодовой базе продукта компании, а также к внутреннему ноу-хау и «недокументированным» сведениям коммерческого характера, связанным с продуктом. В результате такого доступа под NDA у представителей покупателя могли сохраниться «остаточные знания», связанные с разработкой продукта сторонней компанией. Такие знания при этом нельзя назвать конкретной технической, финансовой или иной ценной объективно выраженной информацией или ОИС. Они, скорее, относятся к идеям, методам, концепциям, обобщениям. «Остаточные знания» — это то, что команда покупателя непосредственно запомнила в процессе анализа кода или инфраструктуры приобретаемой компании, но при этом такие сведения максимально абстрагированы от информации, охраняемой NDA.

Покупатель, особенно если он является конкурентом приобретаемой компании, может быть заинтересован в том, чтобы его команда, получив такие «остаточные знания», могла их свободно использовать в личных и иных целях (в том числе в работе) в случае срыва сделки и чтобы такое использование не являлось нарушением NDA. Продавец может разрешить использование остаточных знаний при условии, что компания не допускала нарушения NDA.

Однако использование «остаточных знаний» может повлечь для покупателя риски нарушения NDA. Чаще всего «остаточными знаниями» считаются те сведения, **которые человек запомнил непроизвольно**, без их фиксации на материальном или ином носителе. Доказать, что запомнившаяся идея была сохранена только «в голове», а не после ее фиксации на бумаге или в компьютере, очень сложно. Если у покупателя не получится это опровергнуть (при условии, что продавец доказал обратное), существует риск прямого нарушения NDA.

В российской практике по сделкам Tech M&A, несмотря на достаточно высокий процент положительных ответов по итогам опроса, **оговорки об остаточных знаниях используются крайне редко**. Во-первых, будет сложно доказать, что конкретная идея, источником которой являются остаточные знания, была «получена» именно в результате технической проверки ПО конкретной компании. Во-вторых, большинство сведений, составляющих «остаточные знания», не являются охраноспособными, а также не могут быть предметом соглашения о конфиденциальности, поскольку их сложно объективировать. В-третьих, как отмечено выше, доказать, что раскрытая информация является «остаточными знаниями», а не запрещенными к распространению сведениями, практически невозможно, что делает этот инструмент скорее рискованным для покупателя. Для продавца такие оговорки также скорее предоставляют некий психологический комфорт, чем реальную защиту от использования представителями покупателя неявно сохранившихся у них знаний и навыков в своих целях, в силу сложности доказывания разграничения «остаточных знаний» и запрещенной к распространению информации.

> **Несмотря на благую цель оговорок «об остаточных знаниях», они фактически не работают. По причине крайне «эфемерного» характера такой оговорки ее использование скорее усложняет отношения сторон сделки. Тем более на стадии преддоговорных отношений, когда при согласовании рамочных договоренностей любое излишнее и тем более непонятное условие может вызвать негативную реакцию ключевых стейкхолдеров сделки.**



Роман Головацкий

партнер

DÉNUO

Как правило, оговорка об «остаточных знаниях» (residual clause или residual information clause) в M&A сделках предполагает возможность использования покупателем информации, ставшей известной ему в силу того, что он получил доступ к ней в процессе due diligence, и сохранившейся в «естественной памяти» сотрудников или представителей покупателя, то есть без использования записей или иных технических средств. В отношении такой информации могут не применяться ограничения, установленные соглашением о неразглашении (NDA).

Основным аргументом в пользу включения в NDA оговорки об «остаточных знаниях» является сложность разграничения информации, полученной в связи с конкретной сделкой, от информации, которая была известна или усвоена ранее.

Между тем проблематичность таких оговорок заключается в том, что для продавца будет сохраняться риск их расширительного толкования, а покупатель столкнется с практическими сложностями доказывания того, что информация была запомнена «естественным путем», а не скопирована намеренно.

3 Юридическая специфика сделок M&A с ИИ-компаниями



Раздел 1

Периметр ключевых активов ИИ-компаний в контексте M&A

АВТОРЫ



Анастасия Нерчинская



Александр Панов
VERBA LEGAL



Роман Головацкий
DENUO



Анатолий Земцов
DFCenter



Шермет Курбанов
SL Legal

Краткие выводы

- Для оценки и структурирования сделки M&A в отношении ИИ-компании покупателю важно корректно определить периметр ключевых ИИ-активов и их юридическую принадлежность. Анализ сделок с ИИ-компаниями по итогам 2025 г. показал, что наиболее значимыми ИИ-активами таких бизнесов являются наборы данных, используемых для адаптации модели, библиотеки системных промптов, а в некоторых случаях — ИИ-модель, если она носит уникальный характер для конкретного прикладного решения.

- В основе ИИ-системы чаще всего лежит сторонняя базовая модель. Право ее использования, включая возможность дообучения, предоставляется разработчику ИИ-системы на основе договора, тип которого зависит от формата распространения модели. Обычно — это лицензионный договор, заключаемый с разработчиком(-ами) модели путем акцепта стандартизированной публичной оферты. Модель во многих случаях может быть заменена на другую, поэтому далеко не всегда она является ключевым ИИ-активом.

- В России в 2025 г. начал активно развиваться тренд на локализацию и русификацию ИИ-решений, который будет ожидаемо усиливаться в 2026 г. по мере разработки Законопроекта Минцифры и появления других регуляторных инициатив. Возрастет ценность ИИ-систем, использующих локализованный модельный стек и обеспечивающих обработку данных на территории РФ, а также — рост числа on-premise форматов развертывания моделей.



Илья Булгаков
DENUO

- Уникальность и коммерческая ценность ИИ-системы в существенной степени определяется слоем данных, который контролирует ее разработчик. Через управление данными обеспечивается влияние на поведение интегрированной в ИИ-систему модели. Для целей M&A сделки слой данных следует рассматривать как один из ключевых объектов анализа.

- Правовая квалификация дообучающих датасетов и вопросы, связанные с правовым титулом в их отношении, на сегодняшний день остаются неоднозначными. Подтверждение правового режима датасета как базы данных, охраняемой смежным правом, — длительный и дорогостоящий процесс, требующий привлечения технических экспертов и специалистов по оценке данных.

- При подготовке транзакционной документации следует учитывать, что у дообучателя модели не возникает самостоятельного правового титула (исключительного права) на результат ее дообучения. Пределы прав его использования определяются главным образом условиями соглашения с владельцем базовой модели.

- Большинство ИИ-систем используют архитектурный шаблон RAG — комплексный актив, включающий разнородные элементы, каждый из которых может иметь отдельный правовой режим. Существенное значение имеет наличие у создателя ИИ-системы правовых оснований для использования материалов, входящих в базу знаний RAG, отсутствие которых может повлечь нарушение исключительных прав их законных обладателей.

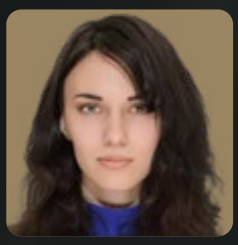
- Применительно к активам оркестрационного слоя ИИ-системы важное значение имеют библиотеки системных промптов. Разработчик ИИ-систем должен обеспечить наличие правового основания их использования.

Чтобы определить стоимость ИИ-бизнеса и правильно структурировать сделку по его приобретению, покупателю важно четко определить набор ключевых активов и установить круг их текущих владельцев. Далеко не все компании, использующие в своей деятельности ИИ-инструменты, являются технологическими, и тем более — ИИ-бизнесами. Многие игроки используют ИИ для трансформации и автоматизации бизнес-процессов, создавая собственные ИИ-системы. Однако если эти процессы не влияют на оценку компании, она не становится ИИ-бизнесом. К ИИ-сегменту относятся только те компании, **у которых ИИ-компоненты формируют самостоятельную экономическую ценность, создают денежные потоки и являются ключевой составляющей их стоимости**.

В этом разделе анализируется **периметр активов, формирующих ИИ-системы[21] и сервисы**, составляющие ядро монетизации ИИ-компаний. Позиции и мнения экспертов рынка по наиболее сложным вопросам владения ИИ-активами приводятся в разрезе ключевых архитектурных уровней ИИ-системы — модели, данных, оркестрации. Анализ ИИ-технологии требует послойного изучения всех относящихся к ней активов.

[21] Анализ M&A и VC сделок с ИИ-активами по итогам 2025 г. показал, что в основе стоимости большинства таких бизнесов лежат ИИ-системы.

#РАСПРЕДЕЛЕНИЕ_РИСКОВ_В_M&A



Анастасия Нерчинская

Приобретатели ИИ-бизнесов заинтересованы в том, чтобы компания имела устойчивый и юридически «чистый» титул на ключевые активы. Такая предпосылка закладывается и в оценку бизнеса. На практике анализ ИИ-активов более сложен, чем работа с традиционными ИТ-объектами. Особенность заключается в том, что ИИ-компании (операторы ИИ-систем) чаще всего не являются абсолютным (титульным) владельцем всех ИИ-активов. Продавец такого бизнеса в большинстве случаев[22] не может сказать покупателю, что обладает исключительными правами на все объекты интеллектуальной собственности внутри ИИ-системы. Покупатель же при анализе контура ИИ-активов сталкивается с более существенной информационной асимметрией в отношении технического и юридического «содержания» продукта, чем в сделках с другими видами активов.

[22] Исключение составляют ИТ-экосистемы, в рамках которых сосредоточена вся ИИ-вертикаль, где оператор системы одновременно является разработчиком модели или относится к его корпоративной группе.

1.1 Уровень модели: титул и ограничения

За пределами крупнейших ИТ-экосистем разработчики ИИ-сервисов не имеют собственных базовых моделей. Создаваемые **ИИ-системы чаще всего опираются на внешнюю базовую модель или локализованную «производную» от нее**. При этом если модель сложно быстро заменить или она носит уникальный характер, на этот слой ИИ-системы приходится существенная технологическая, коммерческая и регуляторная нагрузка.

При определении правового режима использования модели в рамках ИИ-системы следует отталкиваться от формата ее распространения[23]: закрытая модель, полностью открытая (open source) или промежуточные варианты (например, open weight).

На момент выхода данного исследования отсутствуют статистические данные о форматах использования ИИ-моделей, преобладающих в 2025 г. среди ИИ-бизнесов, выступающих объектами сделок VC и M&A. При этом многие эксперты отмечают, что, если ИИ-система создается для решения прикладных задач в сфере оборота «чувствительных» данных (например, медицинских или финансовых) или для целей использования на объекте КИИ, — модель, скорее всего, будет локализована.

Для этого разработчику ИИ-системы потребуется экземпляр весов (параметров) модели. Такая возможность есть при использовании открытых форматов моделей (open source и open weight), а также при локальном (on-premise) развертывании закрытой модели[24].

Если же создается «обычный» SaaS-сервис, то для его эксплуатации могут использоваться и нелокализованные модели.

В России в 2025 г. начал активно развиваться тренд на локализацию и русификацию ИИ-решений, который будет ожидаемо усиливаться в 2026 г. по мере развития Законопроекта Минцифры и других нормотворческих инициатив.

[23] См. описание форматов распространения моделей далее на стр. 391 и стр. 551.

[24] Этот формат используется значительно реже по причине его высокой стоимости.

1.1.1 Правовое основание использования базовой модели

Базовая модель — это основа функционирования любой ИИ-системы. Как было отмечено выше, наиболее часто при создании ИИ-системы используется чужая модель, а право ее использования предоставляется **по договору**. Разработчик ИИ-системы на основе сторонней ИИ-модели должен четко понимать **источник происхождения модели, правовое основание ее использования** и иметь **экземпляр соответствующего договора или условий оферты**.

Условия и правомочия использования модели существенно зависят от того, каким образом разработчик ИИ-системы получил к ней доступ. Существует несколько **основных форматов использования и распространения модели**:

Закрытая модель, предоставляемая как сервис (формат SaaS)

оператор ИИ-системы получает право доступа к модели на основании лицензионного договора[25] / стандартизированной публичной оферты (Terms of Use) разработчика модели. В этом случае пользователь не получает экземпляр весов модели, не имеет права ее изменять и дообучать за пределами функциональности, предусмотренной разработчиком модели.

Закрытая модель, развертываемая локально (формат on-premise)

создатель ИИ-системы на основе соответствующего лицензионного договора с разработчиком модели получает возможность развертывания экземпляра модели на своей инфраструктуре.

Открытая модель, распространяемая свободно

разработчик ИИ-системы получает доступ к экземпляру весов (формат open weight) / к другим артефактам модели (формат open source) путем присоединения к условиям соответствующей открытой лицензии.

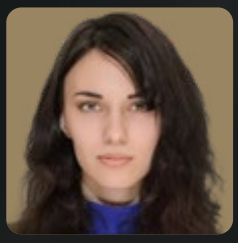
В большинстве случаев внешний пользователь модели (например, разработчик ИИ-системы) **не имеет возможности каким-либо образом повлиять на условия ее использования** и вынужден присоединиться к стандартизированным формам договоров, контролируемым провайдером модели. В индивидуальном порядке условия использования модели могут согласовываться в рамках формата локального развертывания закрытых моделей, что встречается значительно реже.

[25] В некоторых случаях используется договор оказания услуг.

Таким образом, в отношении базовой модели у создателя ИИ-системы **чаще всего есть только ограниченное (не абсолютное) право использования модели в пределах, строго определенных** лицензионным или иным соглашением.

При использовании закрытой модели посредством стороннего API пользователь (создатель системы) не имеет доступа к каким-либо артефактам модели (включая ее веса). Однако важно понимать, что даже наличие экземпляра весов модели при ее использовании в других форматах само по себе **не означает предоставление пользователю исключительного права ни на веса, ни на модель в целом**. Правообладатель модели в этом случае не изменяется, пользователь становится лишь владельцем экземпляра соответствующего объекта (весов, файла с кодом инференса, конфигурационного файла и т. п.).

#РАСПРЕДЕЛЕНИЕ_РИСКОВ_В_M&A



Анастасия Нерчинская

В контексте сделки M&A следует учитывать, что условия лицензий на использование многих ИИ-моделей являются открытыми, и любой гипотетический покупатель соответствующего бизнеса имеет к ним свободный доступ, в том числе для целей анализа в рамках технического или юридического due diligence. К примеру, если покупатель ИИ-компании знает, на какой модели создана ИИ-система, лежащая в основе бизнеса, и если условия ее использования и артефакты (веса, конфигурации, файл инференса и т. п.) находятся в открытом доступе, — такая информация с высокой степенью вероятности будет считаться раскрытой покупателю, а знание о ней — вменено ему, даже если покупатель не ознакомился с текстом договора, не запросил его у продавца или компании или же такие сведения не были ему предоставлены по запросу.

> **В отношении базовой модели у создателя ИИ-системы чаще всего есть только ограниченное (не абсолютное) право ее использования в пределах, строго определенных лицензионным или иным соглашением.**

1.1.2 Ограничения использования модели

В лицензии или ином соглашении об использовании модели содержится основная правовая информация, необходимая для анализа покупателем юридической «чистоты» ИИ-системы. Помимо прочего, в таких документах предусмотрены ограничения и допустимые пределы использования базовой модели, в том числе при ее интеграции в другое решение (например, в систему) и адаптации.

Ключевые условия соглашения об использовании модели, которые покупателю необходимо проанализировать в зависимости от контекста сделки:

- ограничения по целям использования модели, включая допустимость коммерческого использования;
- ограничения по числу пользователей итогового коммерческого продукта, созданного на основе модели;
- дополнительные ограничения по монетизации продукта в целом;
- распределение прав на результаты (генерации), создаваемые моделью;
- распределение прав на обрабатываемые пользовательские данные (промпты, документы, изображения и т. п.);
- возможность дообучения модели третьими лицами;
- распределение прав на результаты дообучения модели;
- ответственность пользователя за «чистоту» входящих данных;
- срок использования модели;
- требования к раскрытию исходного кода модифицированного решения, созданного на основе модели, включая результаты дообучения модели, или решения, в которое интегрирована модель;
- требования к совместимости модели с другими решениями;
- условия прекращения действия лицензии (в том числе принудительного) и последствия ее прекращения;
- возможность использования иных артефактов модели помимо весов — кода инференса, архитектуры, гиперпараметров, обучающих данных и т. п.;
- ограничение ответственности разработчика модели.

#АНАЛИЗ_РИСКОВ



Роман Головацкий

партнер

Dénuo

Ключевая специфика большинства бизнесов, построенных на основе ИИ-решений, заключается в их перманентной технической и юридической зависимости от внешних ИИ-моделей, используемых в подобных решениях. Это должен понимать покупатель, намеревающийся приобрести такой бизнес. Титул разработчика в отношении ИИ-решения будет носить ограниченный характер, распространяясь главным образом на собственноручно разработанную часть такого решения, но не на интегрированные в него компоненты третьих лиц. Поэтому при проведении проверки прав требуется оценка не только титула проприетарной части ИИ-решения, но также лицензионных и иных ограничений по использованию соответствующей модели, на основе которой такое решение построено. Последнее особенно важно не только с точки зрения подтверждения правомерности функционирования бизнеса в его текущем формате, но и для целей оценки масштабируемости и возможности перспективного использования ИИ-решения, которое планирует осуществлять покупатель после получения контроля над приобретенным бизнесом.

#РАСПРЕДЕЛЕНИЕ_РИСКОВ_В_M&A

В контексте сделки M&A с ИИ-активом необходимо учитывать, что ответственность разработчика модели практически всегда **ограничена условием «как есть» (as is)**. В том числе исключена ответственность разработчика модели за ущерб, причиненный ее использованием. Поэтому у создателей ИИ-систем (менеджмента и владельцев компании) обычно **отсутствует возможность обратиться к разработчику модели с какими-либо требованиями в связи с ее дефектами или причиненным ущербом**, если иное не предусмотрено законодательством.

В текущей версии Законопроекта Минцифры предусмотрено право оператора ИИ-системы обратиться с регрессным требованием к поставщику «некачественной» ИИ-технологии, что также подразумевает разработчика модели. Однако поскольку в базовом сценарии создатель ИИ-системы не имеет каких-либо гарантий от разработчика модели, это влияет на объем и характер собственных гарантий при продаже бизнеса на основе ИИ-системы, в котором использована чужая ИИ-модель.

Соответствующие риски **в существенной степени относятся к системным (архитектурным), зависящим преимущественно от разработчика модели**, и не могут быть перенесены исключительно на создателя ИИ-системы посредством транзакционных инструментов. При этом следует учитывать, что «безопасное поведение» модели в определенной степени зависит и от действий самого продавца (создателя ИИ-системы).

1.1.3 Тренд на локализацию ИИ-моделей

В 2025 г. более актуальным стал вопрос локализации и адаптации ИИ-моделей к отечественным регуляторным требованиям. По мере развития российского регулирования сферы ИИ[26] возрастет ценность ИИ-систем, использующих локализованный стек ИИ-моделей, обеспечивающих обработку данных на территории РФ, в отношении которых может быть подтверждено отечественное происхождение датасетов и их соответствие требованиям качества и безопасности.

> **Наличие у пользователя экземпляра весов модели само по себе не означает предоставление ему исключительного права ни на веса, ни на модель в целом.**

С учетом развития этого тренда уже на этапе создания ИИ-систем и сервисов участникам рынка следует задумываться о выборе модели с допустимым правовым режимом и реализации комплекса мер, направленных на снижение регуляторных, технологических и репутационных рисков. Важное значение будет иметь не только наличие «чистого» правового основания для использования модели, но и **степень технологической и юридической автономности всего модельного стека** (включая веса, инференс-контур, адаптеры дообучения, эмбеддинги RAG, оркестрационный слой, фильтры и параметры безопасности).

В связи с развитием этой тенденции закономерно ожидается рост числа on-premise ИИ-решений (прежде всего, это форматы использования модели open source и open weight). Для сервисов, обрабатывающих персональные данные граждан РФ или эксплуатируемых на объектах КИИ, использование зарубежных моделей не будет соответствовать регуляторным требованиям. Это следует учитывать при планировании сделки по продаже ИИ-компании.

[26] Включая Законопроект Минцифры, предусматривающий категории суверенной, национальной и доверенной ИИ-модели, для госсектора, сферы КИИ и B2B-сегмента «чувствительных» данных. При этом важно отметить, что для участников исключительно B2B- и B2C-секторов предусмотренные Законопроектом Минцифры требования к использованию ИИ не являются обязательными.

1.1.4 «Следы» обучающих данных в слое модели

Вопрос о том, содержит ли модель в каком-либо виде обучающий датасет или его фрагменты, является одним из самых сложных и дискуссионных. Он имеет конкретное практическое значение, поскольку влияет на объем рисков, связанных с ИИ-моделью, которые могут «перетекать» в прикладные ИИ-решения и подходы к их распределению между сторонами сделки.

Некоторые эксперты рынка отмечают, что предобучающие датасеты или их элементы не содержатся «в корпусе» моделей и являются полностью автономными по отношению к ним активами.

#ПРАВОВОЙ_РЕЖИМ



Анна Максименко

партнер

KKMP LEGAL

С правовой точки зрения обучающий датасет — автономный актив, который остается таковым, в том числе после обучения модели. Его правовой режим определяется наличием признаков объекта интеллектуальной собственности (отдельных произведений или базы данных), а не местом технического хранения. Его использование для обучения, особенно в коммерческих целях, порождает риски нарушения интеллектуальных прав, что подтверждается множеством судебных разбирательств по всему миру. Ключевые вопросы сосредоточены не в техническом «встраивании» данных в модель, а в законности их изначального сбора и способности модели воспроизводить охраняемые элементы из обучающего датасета.

#ПРАВОВОЙ_РЕЖИМ



Артем Никифоров

ведущий юрисконсульт Управления интеллектуальной собственностью

Яндекс

Под обучающим датасетом можно иметь в виду довольно различные моменты, но одно можно сказать точно: так как в ИИ попадают только корреляции, идеи и принципы, нельзя говорить о том, что ИИ хранит в себе обучающие данные.



Анатолий Земцов

управляющий партнер

dfcenter

Обучающий датасет не «хранится» внутри модели в прямом виде. В модели сохраняются только параметры (веса), являющиеся результатом обучения. Поэтому датасет остается самостоятельным активом, который может использоваться повторно, дополняться или передаваться (отчуждаться) отдельно. С правовой и коммерческой точки зрения это автономный объект.

С технической точки зрения утверждение о том, что модель не содержит обучающий датасет в его исходном виде, является корректным. Однако в контексте возможных юридических рисков этот вопрос порождает сложную дискуссию, развитие которой можно наблюдать на площадках некоторых зарубежных ИИ-регуляторов. Суть проблемы сводится к следующему — существует точка зрения, что, несмотря на всю глубину преобразований, персональные данные и объекты интеллектуальной собственности способны «условно» сохраняться в модели, и при определенных условиях, включая корректно сформулированный запрос, могут быть извлечены из нее и воссозданы.

> **С учетом развития тренда на локализацию и русификацию моделей участникам рынка уже на этапе создания ИИ-систем следует задумываться о выборе моделей с допустимым правовым режимом и реализации комплекса мер, направленных на снижение регуляторных, технологических и репутационных рисков.**

В связи с этим утверждение о том, что модель «напрямую» не хранит обучающие данные, не снимает риска, пусть и гипотетического, связанного с возможностью дословного или почти дословного воспроизведения охраняемых материалов в выдаваемых моделью результатах. Такое воспроизведение может свидетельствовать о том, что соответствующие фрагменты объективно присутствуют в параметрах модели в форме, достаточной для их реконструкции даже без специального указания на них в промпте.

Более подробно об этой проблеме рассказали **Шермет Курбанов (SL LEGAL) и Анастасия Нерчинская**.

#АНАЛИЗ_РИСКОВ



Шермет Курбанов

соруководитель практики интеллектуальной собственности и цифрового права

sll
SL LEGAL

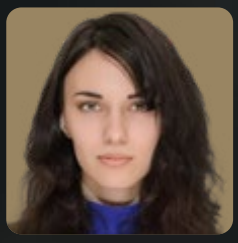
Технически модель изучает закономерности в данных, чтобы генерировать принципиально новый контент, не храня сам датасет. Это подтверждает простой расчет: обучающая выборка может занимать сотни терабайт, тогда как итоговая модель — лишь гигабайты.

Вместе с этим модель может «запоминать» конкретные материалы из обучающей выборки. Сторонники защиты интеллектуальной собственности определяют это так: если модель без явного указания в промпте способна выдать дословную или практически идентичную копию охраняемого материала, это служит доказательством, что материал существует в какой-то форме в весах модели.

Их оппоненты настаивают, что в весах модели хранятся лишь абстрактные математические преобразования, а не читаемая копия произведения. Им возражают: важна не техническая реализация, а функциональная возможность реконструировать произведение.

Таким образом, дискуссия смещается из плоскости чистой технологии в сферу интерпретации: что считать «воспроизведением» произведения — его физическое «присутствие» в параметрах модели или саму возможность его реконструировать.

#РАСПРЕДЕЛЕНИЕ_РИСКОВ_В_M&A



Анастасия Нерчинская

Модель хранит не копии обучающих данных, а математические закономерности и паттерны, извлеченные из них. Но именно эти «слепки» данных в ряде случаев позволяют посредством использования модели реконструировать оригинальный объект с точностью, достаточной для признания факта его воспроизведения. Это — системный риск, который потенциально применим к любой современной ИИ-модели, интегрированной в прикладное ИИ-решение. Митигировать его конкретными инструментами (например, пытаясь исключить «проблемные» веса) практически невозможно. Такое воспроизведение является следствием глубины запоминания модели, а не локализованным багом, который поддается детекции и корректировке при разумных усилиях.

Поэтому в рамках сделки M&A с ИИ-бизнесом нужно аккуратно подходить к работе с такими рисками. При проведении due diligence ни продавец, ни тем более покупатель в абсолютном большинстве случаев не смогут получить доступ к предобучающему датасету модели и проверить наличие согласий (авторизаций) на использование в модели каждого потенциально охраняемого объекта.

Некоторые полностью открытые модели раскрывают и обучающие датасеты, в этом случае у создателя ИИ-системы есть гипотетическая возможность с помощью технических методов выявить в массиве данных охраняемые объекты. Однако проверка получения разработчиком модели согласий у правообладателей таких объектов, в том числе для целей обучения модели, или наличия иного законного основания их использования представляется заведомо невыполнимой задачей. Даже если проводить такой due diligence несколько месяцев с участием огромной команды юристов. Поэтому указанный выше риск, связанный с «наследованием» данных модели, является системным, архитектурным и не может быть полностью перенесен на продавца (владельца ИИ-системы).

При приобретении ИИ-актива для определенных целей покупателю следует провести валидационное тестирование системы на релевантной для его бизнеса выборке данных, чтобы оценить частоту и характер воспроизведения потенциально охраняемого контента. И, если в рамках тестовой выдачи ответов будет выявлена систематическая генерация объектов, «похожих» на чужую интеллектуальную собственность или персональные данные (при отсутствии явного указания на них в промптах), покупателю следует попросить продавца раскрыть известные ему детали о примененных методах фильтрации, возможностях дообучения модели и прочих опциях снижения такого риска. На основе полученных данных покупатель может оценить, является ли уровень риска для него приемлемым, либо принять решение об отказе от сделки.

Само по себе требование к продавцу ИИ-компании дать заверение об отсутствии оснований для материализации подобных «наследуемых» рисков или попытка полностью переложить на продавца этот риск иными транзакционными инструментами, на мой взгляд, необоснованны. Продавец не является «лучшим» носителем этого риска, и если он сделал «все, что мог», чтобы его снизить, например, установил блокировку запросов, направленных на извлечение охраняемого контента, внедрил механизмы постобработки генерации объектов, «похожих» на охраняемые, применил инструменты перефразирования или исключения «подозрительных» фрагментов и т. п. — он не может отвечать перед покупателем за реализацию такого риска.

Таким образом, риск «технического запоминания» моделью данных, на которых она обучалась, является неотъемлемым для любой модели и не может быть полностью митигирован на уровне архитектуры или постобработки без существенного ухудшения качества генерации. Дополнительную сложность создает распространение проблемы на любой тип данных (модальность) — аудио, видео, графика, текст, код. С точки зрения правовой квалификации, ключевое значение приобретает не способ хранения информации внутри модели, а **функциональная возможность воссоздания произведения при использовании модели (хотя точка в этом вопросе все еще не поставлена)**.

Следовательно, распространение модели (в том числе путем копирования весов), способной при обычных условиях эксплуатации генерировать идентичные или практически идентичные копии охраняемых объектов, может рассматриваться как действие, влекущее риски нарушения исключительных прав, независимо от факта отсутствия в весах модели «читаемой копии» исходного датасета.

1.2 Слой данных: вопросы владения и использования

Слой ИИ-модели очень важен в контексте анализа периметра активов ИИ-системы, поскольку в нем концентрируется ИИ-составляющая всего решения. Однако уникальность и, в первую очередь, конкурентные преимущества ИИ-продукта сосредоточены в сфере данных.

На уровне слоя данных ИИ-системы центральное значение имеют **качество** (репрезентативность, релевантность, объем) **датасетов**, на которых дообучается или донастраивается модель, **их правовой режим** (включая вопросы титула), а также **юридическая «чистота»**, в том числе возможность их использования в коммерческом продукте[27]. Массивы данных являются критически важным активом, формирующим конкурентные преимущества ИИ-бизнеса.

Для большинства прикладных ИИ-сервисов именно уровень данных определяет степень уникальности продукта, адаптации к отраслевой задаче, локальному языковому контексту, пользовательским сценариям, соответствия требованиям к точности и безопасности результата. За исключением некоторых категорий датасетов[28] слой данных практически полностью контролируется создателем ИИ-системы. Именно через него он **может в определенной степени влиять на поведение чужой модели**, интегрированной в систему.

Далее приведен обзор мнений ведущих экспертов рынка об особенностях правового режима различных наборов данных, которые используются при создании и эксплуатации ИИ-систем.

[27] В рамках исследования мы не фокусировались на технических аспектах данных (к которым относятся упомянутые характеристики качества датасетов). Однако следует отметить их первостепенную важность для оптимальной работы ИИ-продукта.

[28] В первую очередь, предобучающих датасетов, которые контролирует разработчик модели, но не создатель ИИ-системы.

1.2.1 Категории данных внутри ИИ-системы

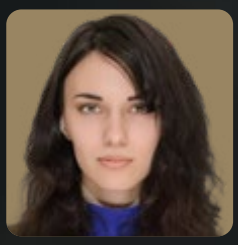
Для целей сделки M&A слой данных является одной из приоритетных областей due diligence и сферой концентрации усилий по митигации рисков. Важно учитывать, что данные, используемые в ИИ-системе, — это не некий единый однородный массив, а совокупность различных контуров информации и артефактов, имеющих различный правовой режим и инвестиционную ценность. К ним могут относиться, в частности:

- **Обучающие выборки**, включая **датасеты для «тонкой настройки» модели** (Fine-Tuning). Крайне важно отличать выборку, используемую для дообучения модели в процессе ее адаптации при создании системы, и не смешивать это понятие с предобучающим датасетом.
- **Валидационные и тестовые** наборы данных.
- **Пользовательские данные**, собираемые в процессе эксплуатации ИИ-системы.
- Данные для работы **систем извлечения и дополнения контекста** (RAG).
- **Синтетические данные**, создаваемые самой компанией или по ее заказу.

> **Ни продавец, создавший ИИ-систему, ни тем более покупатель в абсолютном большинстве случаев не смогут получить доступ к предобучающему датасету базовой модели и проверить наличие согласий (авторизаций) на использование в рамках модели каждого потенциально охраняемого объекта при проведении due diligence.**

Следует различать, какими именно массивами данных ИИ-компания владеет, а какие лишь обрабатывает без возникновения у нее прав на дальнейшее самостоятельное использование и коммерциализацию.

#РАСПРЕДЕЛЕНИЕ_РИСКОВ_В_M&A



Анастасия Нерчинская

В контексте сделки M&A с ИИ-бизнесом важное значение имеет уровень организации процедур и процессов, связанных с созданием и эксплуатацией ИИ-системы. Без четко выстроенной системы документирования и мониторинга параметров ИИ-системы продавец не сможет обосновать, что относится к его зоне контроля, а что — к предпринимательскому риску покупателя, раскрыть значимые характеристики поведения ИИ-модели и показать «точку отсчета» собственного влияния на их динамику, обеспечить разумный баланс при распределении рисков и правильно ответить на запрос покупателя о предоставлении гарантий, связанных с юридической «чистотой» ИИ-решения. Все это в наибольшей степени относится к слою данных, обрабатываемых ИИ-системой.

ИИ-компаниям целесообразно внедрить систему управления жизненным циклом всех массивов данных и информационных слоев, от которых зависит функционирование ИИ-системы: обучающие, валидационные, тестовые датасеты, пользовательские данные, статические и динамические базы знаний, синтетические данные, выборки для пентестов, оценки безопасности и качества модели и т. п.

В отношении каждого массива данных важно учитывать:

- источник происхождения;
- метод получения;
- правовое основание сбора и обработки;
- наличие ограничений на использование;
- наличие персональных данных, включая специальные или «чувствительные» категории;
- наличие охраняемого контента третьих лиц, в том числе объектов интеллектуальной собственности или информации, составляющей охраняемую законом тайну;

- срок хранения каждой категории данных;
- правила доступа;
- порядок обновления и удаления данных;
- инструкции и ограничения использования данных для обучения модели.

В контексте сделок M&A с ИИ-бизнесами наличие отлаженной системы управления и учета различных наборов и массивов данных позволяет решить ряд важных задач. Во-первых, как для продавца, так и для покупателя это облегчает процесс проведения юридической, технической и ИБ-проверки значимых для ИИ-системы потоков и массивов данных.

Во-вторых, такая система может быть полезным инструментом раскрытия информации на стороне продавца, в том числе против запрашиваемых покупателем заверений. Предоставление покупателю сведений в отношении управления данными (например, о необходимости использования в ИИ-системе только данных определенного формата или полученных из конкретных источников) частично переносит риски, связанные с data-driven поведением ИИ-модели, на покупателя.

Если же продавец согласился индемнифицировать какие-либо риски возникновения инцидентов, связанных с ИИ, наличие системы управления данными позволяет ему определить и обосновать, возник ли триггер до или после интеграции ИИ-системы в контур покупателя, есть ли связь между инцидентом и изменением среды эксплуатации системы, кто за это отвечает. Наличие у продавца набора эталонных данных и их характеристик, мониторинг отклонения параметров данных в системе, журналирование инцидентов и мер реагирования дает продавцу больше возможностей доказать (или как минимум перенести бремя доказывания соответствующего обстоятельства на покупателя), что инцидент вызван не скрытым дефектом актива, а, например, изменением входного потока данных, их типа или источника в контуре покупателя.

При анализе слоя данных в контексте вопросов правового титула владельца ИИ-системы важно фокусироваться на следующих аспектах:

Титул и его чистота

- Какими **правами** обладает компания на соответствующие массивы данных и есть ли уязвимости у такого владения?
- Какие права возникли у владельца системы на **результат дообучения** модели?
- На каком **правовом основании** компания собрала, приобрела или иным образом получила доступ к соответствующим массивам данных?

Ограничения

- Допускает ли правовой режим соответствующих наборов данных их **использование** для целей дообучения, «тонкой настройки» модели, ее тестирования и коммерческую эксплуатацию?
- Существуют ли **ограничения** для масштабирования ИИ-системы, включая ее интеграцию в объекты в «чувствительных» отраслях?

Контроль

- Есть ли у оператора системы реальная возможность **удалить** датасеты или их часть и понимание, как это может повлиять на работу всей системы?

Ответы на многие из этих вопросов лежат в юридической плоскости. Они определяют уровень юридической «чистоты» и устойчивости правового основания владения данными как ключевым активом ИИ-бизнеса. При этом в рамках сделок M&A с ИИ очень важно правильно **определить границу, по которой влияние создателя системы на поведение модели отделяется от сферы воздействия разработчика модели**. Этот водораздел проходит именно через слой данных ИИ-системы.

1.2.2 Активы и инструменты, используемые при дообучении модели

Существует несколько способов адаптации модели при создании различных ИИ-систем. Некоторые из них предполагают **дообучение модели**, в результате которого полностью или частично изменяются веса модели (например, метод «тонкой настройки»). Остальные, такие как промпт-инжиниринг, RAG-надстройка и ряд других — **не являются методами дообучения** и не приводят к параметрическим изменениям модели. Для целей сделки M&A вопросы титула на различные наборы данных целесообразно рассматривать именно с точки зрения способов их использования при создании ИИ-системы.

> **Уровень данных определяет степень уникальности продукта, его адаптации к отраслевой задаче, локальному языковому контексту, пользовательским сценариям. Через управление слоем данных разработчик ИИ-решения может влиять на поведение чужой модели, интегрированной в систему.**

Если компания планирует дообучать чужую модель, она должна обладать как минимум следующим набором активов и правомочий:

1. Право дообучения модели

Такое право предоставляется разработчику ИИ-системы на основе договора. Существует несколько основных форматов взаимодействия с моделью в процессе ее дообучения.

Закрытая модель

- Основа процесса дообучения — право доступа к API модели на основании лицензионного договора, в том числе заключаемого посредством акцепта публичной оферты владельца базовой модели (SaaS-формат). В этом случае разработчик ИИ-системы (дообучатель модели) не получает экземпляра весов, взаимодействие с моделью и ее дообучение происходит через API-шлюз на инфраструктуре ее разработчика. В этом случае оператор системы **полностью зависит от персонала, инфраструктуры и вычислительных ресурсов разработчика модели**. Однако это позволяет не перегружать свой ИТ-контур и дообучать модель без привлечения соответствующих мощностей.

  В этом случае создатель ИИ-системы «**не видит» сам процесс дообучения**, а также **не имеет доступа к экземпляру «дообученных» (измененных) весов** модели и пользуется ими также посредством API. Он лишь загружает свои данные в инфраструктуру модели, которые затем обрабатываются алгоритмами

разработчика модели. То есть сам процесс дообучения осуществляет оператор модели. Создатель ИИ-системы выступает в качестве заказчика услуг (как бы ни назывался договор) и имеет только право на «результат» оказания таких услуг в виде функционала дообученной на его данных модели.

- Разработчик ИИ-системы может развернуть экземпляр весов закрытой модели **на своей инфраструктуре** (on-premise-формат) и дообучать модель самостоятельно. Для этого необходимо, чтобы лицензия предусматривала право на дообучение модели, возможность развертывания как модели, так и результата дообучения в контуре лицензиата.

#АНАЛИЗ_РИСКОВ

При использовании закрытой модели, вне зависимости от формата доступа, важно проверить:

- наличие у ИИ-компании полномочий на заключение договора с разработчиком модели и их реализацию с соблюдением надлежащей формы (например, действующая учетная запись, используемая при приобретении прав доступа к модели, должна быть оформлена на имя приобретаемой компании, а не являться личным аккаунтом ее работника);
- срок действия соответствующей лицензии или договора оказания услуг;
- возможные ограничения и спецификации, связанные с дообучением модели (формат и категории данных, цели дообучения, особенности развертывания в контуре заказчика и т. п.);
- распределение прав на результат дообучения и на данные, используемые для дообучения;
- для формата доступа через API — максимальный режим обеспечения бесперебойного сервиса в соответствии с SLA[29] и контроль риска внезапного отключения функционала модели;
- отсутствие ограничений на коммерциализацию дообученной модели, в том числе интегрированной в ИИ-систему.

[29] Services Level Agreement (соглашение об уровне сервисного обслуживания).

Открытая модель

Право на дообучение должно быть прямо указано в открытой лицензии на соответствующую модель (open source) или специальной лицензии на веса модели (open weight). В этом случае разработчик ИИ-системы получает прямой доступ к файлу с весами и конфигурациям базовой модели (как в формате open source, так и open weight) и может развернуть модель на своей инфраструктуре. Это предоставляет ему автономность от инфраструктуры и персонала базовой модели, но требует наличия собственных (или арендованных) мощностей и экспертизы, что существенно повышает затраты на дообучение модели.

> **В рамках сделок M&A с ИИ очень важно правильно определить границу, по которой влияние создателя системы на поведение модели отделяется от сферы воздействия разработчика модели. Этот водораздел проходит преимущественно через слой данных ИИ-системы.**

При использовании открытой лицензии в отношении экземпляра весов или иных артефактов модельного стека особое значение имеют ее условия в части требований к коммерческому использованию и указанию авторства.

---

2. Обучающий датасет

Это ключевой актив. Зачастую массивы данных для целей дообучения модели представлены узкоспециализированными, нишевыми, тщательно подготовленными выборками, объем которых, однако, существенно меньше, чем у предобучающих датасетов модели.

3. Алгоритм обучения модели

А также его настройки и модификации, описание архитектуры дообученной модели (в той части, в которой она отличается от базовой).

4. Слой оркестрации

Оркестрация, включая функцию промпт-инжиниринга, обеспечивает взаимодействие модели в рамках ИИ-системы с разными контурами пользователей. Зачастую ключевой актив здесь представлен набором системных промптов. При использовании открытых весов от качества системных промптов и их конфиденциальности существенно зависит коммерческая ценность итогового продукта.

5. Наборы данных (базы знаний) и созданные на их основе векторные базы данных

Являются важным активом в составе ИИ-системы, если она использует RAG-надстройку или иные методы адаптации модели, не связанные с ее дообучением.

6. Второстепенные активы

Традиционное ПО, включая инструментарий разметки данных, создания эмбеддингов, системы управления базами данных, а также реляционные и векторные базы данных.

7. Функция по подготовке данных (R&D)

Если для целей дообучения модели компания готовит датасет собственными силами, такая функция — важный актив. Это актуально и в случаях, когда компания локализует модель и дообучает ее на своей инфраструктуре, и когда загружает данные через API в контур владельца модели. Если же компания приобретает сторонние датасеты, степень важности этой функции снижается.

В процессе полного дообучения модели изменяются все ее веса, при этом задействуется крупный массив обучающих данных[30]. Эти данные должны быть «чистыми» как с правовой точки зрения, то есть не содержать неавторизованных объектов интеллектуальной собственности, персональных данных и иных объектов с ограниченным доступом (например, охраняемых в режиме банковской или коммерческой тайны), так и с технической.

[30] который тем не менее всегда будет существенно меньше предобучающего датасета.

1.2.3 Титул на обучающие датасеты

При приобретении бизнеса, монетизирующего ИИ-систему на основе дообученной модели, покупателю важно понимать, **на каком основании приобретаемая компания владеет обучающими датасетами**, и насколько такое основание юридически «прочно». Ценность ИИ-системы создается преимущественно за счет нового уникального массива данных, перенастройки весов и более глубокой специализации ИИ-модели.

Большинство экспертов сходятся во мнении, что крупные массивы данных, включая используемые для полного дообучения модели (Full Fine-Tuning), могут охраняться **исключительным правом изготовителя базы данных как объекта смежных прав** (ст. 1333 ГК РФ). Если разработчик ИИ-системы сам организовал создание такого датасета, включая сбор, обработку и расположение данных, **он может считаться ее изготовителем**, обладающим исключительным правом на соответствующую базу данных.

Такой режим правовой охраны возникает лишь при условии, что создание базы данных потребовало существенных финансовых, материальных, организационных или иных затрат. Поэтому **разработчику ИИ-системы целесообразно обеспечить наличие убедительных доказательств (например, экспертных заключений) существенности затрат, понесенных при создании базы данных**. В противном случае наличие у него титула (смежного права изготовителя базы данных) на датасет будет под вопросом.

Более сложной представляется ситуация, когда создатель ИИ-системы не является непосредственным изготовителем базы данных, а приобрел права на нее у третьего лица. Чем дальше разработчик ИИ-системы в цепочке переходов прав от первичного изготовителя базы данных, **тем сложнее ему будет доказать существенность затрат, понесенных при ее создании, и, соответственно, наличие у него титула**. В таких случаях создателю ИИ-системы целесообразно запросить соответствующие доказательства от прежнего правообладателя, например, в рамках договора об отчуждении исключительного права изготовителя базы данных.

> **Большинство экспертов сходятся во мнении, что крупные массивы данных, включая используемые для полного дообучения модели (Full Fine-Tuning), могут охраняться исключительным правом изготовителя базы данных как объекта смежных прав.**

Исключительное право изготовителя базы данных предоставляет его обладателю **монополию на извлечение и использование материалов** этой базы по своему усмотрению. В первую очередь, только обладатель исключительного права может извлекать **существенные массивы данных** — то есть все или большую их часть, что имеет принципиальное значение при использовании технологий ИИ и больших данных (Big Data). Третьи лица не вправе этого делать без разрешения обладателя исключительного права на такую базу данных.

Проблема устойчивости титула

Покупатель бизнеса, в основе которого лежит дообученная ИИ-модель, заинтересован в том, чтобы дообучающий датасет был включен в периметр сделки, а компания имела на него устойчивое правовое основание владения и использования. С позиции инвестора **исключительное право изготовителя базы данных — наиболее полный правовой титул** на обучающий датасет. Однако здесь существует проблема правовой неопределенности.

В рамках текущего правового регулирования больших массивов данных ни сама компания,

ни любое другое лицо **не могут с точностью верифицировать и подтвердить наличие титула** (исключительного права изготовителя базы данных) на крупный датасет. Чтобы заявить о наличии исключительного права, «очищенного» от высоких рисков оспаривания, владелец массива данных должен быть уверен в том, что датасет действительно является базой данных, охраняемой смежным правом.

Как упоминалось ранее, чтобы массив данных мог быть квалифицирован как объект смежного права, его владелец должен доказать факт **несения существенных затрат** на его изготовление, даже если датасет создавало третье лицо. **Существенные затраты — оценочное понятие, четкие устоявшиеся критерии существенности судебной практикой пока не выработаны.** Законодательная презумпция о том, что наличие в такой базе не менее 10 тыс. самостоятельных информационных элементов предполагает существенность затрат на ее изготовление, — опровержима.

> **Чем дальше в цепочке переходов прав разработчик ИИ-системы находится от первичного изготовителя базы данных, тем сложнее ему будет доказать существенность затрат, понесенных при ее создании, и, соответственно, наличие у него титула.**

Покупателю бизнеса, использующего крупные массивы данных, сложно в рамках due diligence верифицировать правовой режим такого датасета и убедиться в наличии у компании смежного права на него. Это долгий и дорогостоящий процесс, требующий привлечения технических экспертов и оценщиков в области данных. Поэтому продавцу такого бизнеса при подготовке компании к продаже целесообразно самостоятельно обратиться к техническим экспертам и оценщикам за обоснованием существенности затрат на изготовление обучающего датасета. **В рамках технической экспертизы может быть подсчитано точное число самостоятельных информационных элементов** соответствующей базы данных, что позволит подтвердить презумпцию существенности затрат и наличие исключительного права на датасет.

Мы попросили **Анатолия Земцова**, управляющего партнера DFCenter, рассказать о том, можно ли при проведении технической экспертизы датасета верифицировать количество информационных элементов, определить приблизительный размер затрат на создание базы данных, выявить потенциальные нарушения, например, получение данных методом парсинга.



Анатолий Земцов

управляющий партнер

dfcenter

Техническая экспертиза позволяет достоверно определить количество самостоятельных элементов в базе данных, анализируя структуру таблиц, записей и уникальных объектов. Не имеет принципиального значения, сырые это или размеченные данные, здесь важна самостоятельность элементов. Также возможно установить признаки конкретного способа получения данных, включая массовый парсинг. Также, по косвенным признакам, возможно оценить объем вычислительных и трудозатрат на формирование такого датасета.

Существенные затраты на изготовление датасета подтверждаются анализом пайплайна сбора и очистки данных, логов аннотации, используемых инструментов разметки, числа задействованных операторов или вычислительных мощностей. Также учитываются версии датасетов, история обновлений, инфраструктура хранения и обработки. В совокупности это позволяет доказать системный и затратный характер формирования базы. Для такой задачи требуется командная работа ИТ-эксперта и специализированного экономиста-оценщика.

Есть еще два важных аспекта, на которые следует обратить внимание при анализе титульных рисков на датасеты.

1. Правомерность методов парсинга

В российском законодательстве и судебной практике пока нет однозначного ответа на вопрос о допустимости включения в состав баз данных, охраняемых смежным правом, информационных элементов, полученных с помощью т. н. метода парсинга. В первую очередь речь идет о категории данных, сгенерированных пользователями веб-сайтов (User-Generated Content).

Существует точка зрения, что **такие данные не могут быть включены в состав датасетов**. При этом, если при подготовке обучающего датасета компания использует метод парсинга, такие данные с высокой степенью вероятности включают пользовательский контент. Это может повлечь не только регуляторные риски, но и титульные. В частности, **владелец соответствующих данных может запретить компании использовать их в составе датасета и потребовать их исключения**. В результате этого в отношении соответствующей части данных будет прекращен режим охраны смежным правом.

#АНАЛИЗ_РИСКОВ



Илья Булгаков

советник

DÉNUO

В российской судебной практике отсутствует однозначный вывод о том, что владельцам веб-сайтов может принадлежать исключительное право на базы данных, содержащие данные, созданные непосредственно пользователями сайта (так называемый user generated content), а не самим владельцем. Также нет единого подхода к признанию извлечения таких данных, доступ к которым является открытым, нарушением исключительных прав.

Учитывая, что объем данных, извлекаемых, сохраняемых и используемых при обучении ИИ-моделей, обычно достаточно большой и может составлять терабайты данных, существует вероятность, что такие действия могут быть признаны нарушением смежных прав, если такая совокупность данных будет квалифицирована как база данных, а владельцы соответствующих сайтов — их правообладателями.

Тем не менее в российской правоприменительной и судебной практике на данный момент нет однозначного подхода к квалификации базы данных, содержащей информацию, создаваемую непосредственно пользователями веб-сайтов (USG content), как объекта смежных прав. В частности, имеется следующий довод против такой квалификации: для возникновения исключительного права на базу данных как объект смежных прав изготовитель должен понести существенные финансовые, организационные и иные затраты, направленные именно на создание базы данных. Если наполнение базы данных осуществляется пользователями веб-сайта, а владелец сайта лишь администрирует ресурс, затраты на администрирование не могут быть приравнены к затратам на создание базы данных.

2. Прямой доступ к датасету

Сделать техническую экспертизу и проверить качество данных можно только при наличии **прямого доступа** к соответствующему датасету. Это важный аспект, который следует учитывать при анализе периметра активов: покупателю ИИ-компании необходимо убедиться в реальном существовании конкретного обучающего массива данных и проверить его характеристики. Это можно сделать только в том случае, если датасет размещен в ИТ-контуре компании (в том числе на арендованных серверах), но не у третьих лиц, включая аффилированных с таргетом, если у них разный технологический стек или инфраструктурный периметр.

> **В рамках технической экспертизы может быть подсчитано точное число самостоятельных информационных элементов соответствующей базы данных, что позволит подтвердить презумпцию существенности затрат и наличие исключительного права на датасет.**

Указанное дополнительно свидетельствует о невозможности технического анализа предобучающих датасетов чужой модели на предмет их качества и юридической «чистоты». Если владелец ИИ-системы не имеет прямого доступа к соответствующему датасету — провести его полноценную техническую экспертизу с существенной степенью достоверности, в том числе для целей определения количества информационных элементов, невозможно.

#МНЕНИЕ_ЭКСПЕРТОВ



Анатолий Земцов

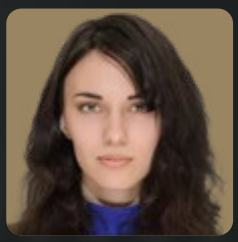
управляющий партнер

dfcenter

При отсутствии доступа к исходному датасету проведение полноценной технической экспертизы для установления количества самостоятельных информационных элементов невозможно. Достоверный подсчет, анализ структуры и исключение дублирования требуют прямого исследования массива данных. Соответственно, лицо, не располагающее обучающими данными чужой модели, не сможет подтвердить их объем и характеристики.

Экспертиза возможна только в отношении тех данных, к которым обеспечен фактический доступ, например в отношении собственного датасета. А без доступа возможен лишь косвенный анализ: исследование поведения модели, совпадений с конкретными источниками, технической документации или следов автоматизированного сбора данных. Однако такие выводы носят вероятностный характер.

#РАСПРЕДЕЛЕНИЕ_РИСКОВ_В_M&A



Анастасия Нерчинская

Слой данных крайне важен для целей формирования контура активов приобретаемой ИИ-компании еще и потому, что именно здесь проходит граница зоны технических и этических рисков модели, интегрированной в систему, за которые уже может отвечать продавец (создатель ИИ-системы), а не разработчик модели.

При приобретении ИИ-компании покупатель может обоснованно запрашивать у продавца гарантии в отношении всего массива дообучающих данных, даже если они приобретены у третьего лица. Оговорки «насколько известно продавцу», переносящие бремя доказывания соответствующих обстоятельств на покупателя, здесь относительно уместны. Качество дообучающего датасета это, за редким исключением, — зона прямого влияния и контроля создателя ИИ-системы (его менеджмента и мажоритарных владельцев, выступающих на стороне продавца).

Предпринимательский риск продавца (владельца бизнеса на основе ИИ-системы) предполагает обеспечение качественной подготовки датасета, включая выполнение требований к его технической и юридической «чистоте». Поэтому здесь вполне допустим подход «вмененного знания» продавца — даже если он не знал, что какие-то данные содержат дефекты, он мог об этом узнать при должной организации процесса их сбора и подготовки на уровне операционной компании. То есть в подавляющем большинстве случаев — это не риск покупателя. Отдельные исключения, связанные с наличием неустранимого (технологического) риска в слое данных, который не может быть полностью перенесен на продавца, например, «чистота» данных при использовании некоторых вариантов динамического RAG, лишь подтверждают общее правило.

При этом такая ситуация совершенно не представляется допустимой в отношении предобучающих датасетов модели. Особенно в тех случаях, когда создатель ИИ-системы использовал закрытую модель через API или открытую в формате open weight. В этих случаях он даже не владеет экземпляром предобучающего датасета и ничего о нем не знает, за исключением информации, публично раскрытой провайдером модели, знание о которой будет автоматически вменяться как продавцу, так и покупателю ИИ-компании. Некоторые исключения здесь могут иметь место при использовании open source формата модели, где иногда раскрыт весь стек, включая предобучающие датасеты, алгоритмы обучения и другие артефакты. Здесь уже набор гарантий продавца в отношении предобучающих данных может обсуждаться более предметно и точечно, но всегда с учетом того факта, что продавец — создатель ИИ-системы — не обучал саму модель на этих данных.

1.2.4 Права на результат дообучения ИИ-модели

Как было отмечено ранее, в результате дообучения базовой модели в той или иной степени могут изменяться ее веса. При полноформатном дообучении могут меняться все веса модели, при ограниченном — только их небольшая часть. В контексте формирования контура приобретаемых активов ИИ-компании возникает ряд практических вопросов, связанных с дообучением сторонней базовой модели:

1. **Какие права на результат дообучения модели возникают у создателя ИИ-системы, в которую интегрирована дообученная модель?**

2. **Кому и на каком основании принадлежит измененная часть весов?**

3. **Возникает ли в результате дообучения производная модель с самостоятельным исключительным правом на нее?**

С технической точки зрения при полном формате «тонкой настройки» (Full Fine-Tuning) модели у дообучателя сохраняется экземпляр ее обновленных весов. А в случае неполного (ограниченного) дообучения (формат PEFT, например, с помощью метода LoRA) — небольшой файл с адаптерами.

Изменение весов модели, полное или частичное, происходит в результате математической оптимизации данных при их обработке с помощью специального алгоритма, а не путем внесения изменений в кодовую базу «руками программиста». В связи с тем, что **такие изменения не носят творческого характера**, возникает вопрос о юридической квалификации результата дообучения модели и о правах, которые возникают у дообучателя на такой объект. Иными словами, можно ли считать, что дообучение чужой модели может привести к созданию производной модели (или иного производного объекта интеллектуальной собственности) с возникновением исключительного права у ее создателя?

Многие эксперты относят этот вопрос **к числу наиболее проблемных в сфере регулирования ИИ**. Большинство из них считает, что в результате дообучения модели не возникает производного объекта. Действия по дообучению **скорее носят характер адаптации ПО**, в результате которой не возникает производного произведения, а у его «автора» — исключительного права на него.

Однако некоторые эксперты считают, что результат дообучения модели может и не являться адаптацией, но при этом он **в любом случае будет являться модификацией ПО, не приводящей к созданию производного произведения** по причине отсутствия творческого характера вносимых изменений.

Мы попросили M&A- и ИТ-юристов прокомментировать эти вопросы и рассказать, какие права могут возникнуть у дообучателя модели в отношении результата ее обучения, а также как они могут соотноситься с правами разработчика модели на такой результат.

#ПРАВОВОЙ_РЕЖИМ



Роман Головацкий

партнер

dénuo

Для того чтобы ответить на вопрос о правах на результат дообучения, в первую очередь, необходимо разобраться с тем, что из себя представляет данный процесс.

По сути, дообучение (fine-tuning) подразумевает перенастройку параметров (весов) чужой (базовой) ИИ-модели на основе своего датасета для достижения конкретных задач дообучателя. Иными словами, это адаптация модели, чтобы на характерных для избранного сценария входных данных она с большей вероятностью выдавала требуемые выходные результаты. При этом, в зависимости от вида fine-tuning, дообучаться может как малая часть параметров (при использовании, в частности, такого метода дообучения как PEFT (Parameter-efficient fine-tuning), так и всех весов сразу (full fine-tuning). Очевидно, что последний вариант возможен лишь при наличии значительных вычислительных ресурсов и данных, он применяется, когда необходима максимальная адаптация модели.

Таким образом, результатом дообучения являются измененные параметры (веса) модели или их обновления, например, в виде отдельных адаптеров. Это именно то, что получает дообучатель в свое распоряжение. Соответственно, ключевым здесь является вопрос о том, какова авторско-правовая природа весов модели. Чаще встречается точка зрения о том, что это часть программы для ЭВМ в виде данных, позволяющих программе функционировать определенным образом. Если исходить из такой парадигмы, то это влечет за собой закономерный вопрос — можно ли считать дообученную модель производным произведением по смыслу ст. 1260 ГК РФ, то есть самостоятельным объектом авторского права? Я придерживаюсь мнения о том, что в рамках текущего правового регулирования это вряд ли возможно, поскольку главным условием охраноспособности произведения с точки зрения авторского права является творческий характер его создания (ст. 1257 ГК РФ). Между тем процесс дообучения, как указано выше, по сути, представляет собой автоматизированную обработку данных, в которой веса определяются

вычислительным процессом, а не творческим выбором человека. Участие человека сводится только к определению задачи и настройке процесса, но не к созданию выраженной формы результата.

Соответственно, полагаю, что у дообучателя не возникает самостоятельного правового титула (исключительного права) на дообученную модель как на производное произведение. Пределы его прав, касающихся использования измененных весов, будут определяться, главным образом, условиями лицензионного соглашения с владельцем базовой модели.

#ПРАВОВОЙ_РЕЖИМ



Шермет Курбанов

соруководитель практики интеллектуальной собственности и цифрового права

SL LEGAL

Дообучение — многозначный термин, используемый на практике в разных значениях: от системного промптинга, создания надстроечной модели с отдельными весами и до обучения изначальной модели с изменением ее весов.

И если мы говорим о последнем — обновлении весов, — вопрос достаточно нетривиальный. Существующее регулирование ПО и баз данных было создано задолго до появления ИИ, поэтому не учитывает его особенностей, в том числе касающихся обучения.

В результате возникает пробел: ИИ-модель развивается по правилам, не предусмотренным и не учтенным в законе. Эта типичная для инноваций ситуация требует глубокого анализа технологии для последующей корректировки регулирования.

На переходный же период индустрия, возможно, будет использовать правовые «костыли», применяя к ИИ режимы наиболее релевантных, но не идеально подходящих объектов. В качестве примера такого подхода можно рассматривать квалификацию дообучения модели как ее модификации в смысле ГК РФ, хотя в отношении применимости этой конструкции к ИИ существует ряд существенных нюансов (в первую очередь, можно ли считать такую модификацию творческой).

Тем не менее, наиболее «приземленный» и приближенный к текущей интерпретации закона подход, по крайней мере на данный момент, — это отсутствие прав на дообученную модель у компании-дообучателя. Основным активом на стороне дообучателя в таком случае является лицензия на базовую модель.

#ПРАВОВОЙ_РЕЖИМ



Артем Никифоров

ведущий юрисконсульт управления интеллектуальной собственностью

Яндекс

Ключевое — договор на базовую модель: разрешено ли дообучение, кому принадлежат новые веса, можно ли распространять результат.

Без согласия правообладателя базовой модели дообучение и тем более публикация могут быть нарушением.

Если дообучение — просто запуск обучения на своих данных без творческого вклада в код / архитектуру, самостоятельные «авторские» права на новые веса возникать не должны — это фактически использование функциональности программы.

Если же дообучающий с согласия правообладателя целенаправленно обучает модель своим творческим трудом, то можно говорить о создании производного произведения. Однако это не означает, что на основе дообученной модели он вправе создавать новые модели (то есть «производные произведения на производные»).

#ПРАВОВОЙ_РЕЖИМ



Елена Полевая

старший юрист

KKMP LEGAL

Права дообучателя на результат дообучения ИИ-модели определяются степенью изменений и условиями лицензии на базовую модель. Если дообучение ограничивается вводом специфических промптов или отдельных гиперпараметров, оно остается в рамках использования по лицензии и не создает у дообучателя новых прав.

Существенные изменения (переобучение на больших данных, модификация архитектуры или кода, создание новых модулей) могут считаться производным произведением или даже новой моделью. Права дообучателя на такую модель регулируются с учетом лицензии на базовую модель. Часто в лицензиях на проприетарное ПО исключительные права на все модификации принадлежат владельцу базовой модели, а дообучатель получает лишь право использования. При этом дообучатель в некоторых случаях может сохранять права на отдельные созданные им элементы, например, на обучающий датасет, исходный код новых компонентов, измененные веса модели. Если же базовая модель распространяется по свободной лицензии, дообучатель обычно получает широкие права на ее модификацию и коммерческое использование результата.

#РАСПРЕДЕЛЕНИЕ_РИСКОВ_В_M&A

Таким образом, даже если владелец ИИ-системы дообучил модель, в том числе путем полноформатной «тонкой настройки», **он не может заявить покупателю бизнеса о наличии у него титула (исключительного права) на производную модель или результат ее дообучения**. Этот аспект важно учитывать при подготовке транзакционной документации при описании оснований владения ключевыми активами, а также в случае запроса покупателем соответствующих титульных гарантий. Право на результат дообучения чужой модели, а также его возможные обременения (например, право разработчика модели использовать результат дообучения на основании неисключительной лицензии) следует описывать со ссылкой на соответствующее лицензионное или иное соглашение (например, договор на разработку) с разработчиком модели.

> **В процессе дообучения базовой модели изменение ее весов, полное или частичное, происходит в результате математической оптимизации данных при их обработке с помощью специального алгоритма, а не путем внесения изменений в кодовую базу «руками программиста». Такие изменения не носят творческого характера и не порождают возникновение производной модели или ее части (весов).**

При этом следует критично оценивать положения о распределении прав в лицензионном соглашении или ином подобном договоре. В первую очередь это относится к положениям, предусматривающим автоматический переход исключительного права на производную модель или результаты ее дообучения лицензиату / заказчику. Как указано выше, в российском правовом поле возможность возникновения самостоятельного правового титула (исключительного права) на результаты дообучения ИИ-модели сегодня подвергается сомнению. В этом смысле классические концепции распределения прав, нередко используемые в подобных договорах в отношении т. н. «предшествующей интеллектуальной собственности» (Background IP) и «вновь созданной интеллектуальной собственности» (Foreground IP), в российском правовом поле могут не иметь юридической силы.

Если в соглашении с разработчиком модели по каким-либо причинам отсутствуют положения о распределении прав на результат ее дообучения или такие правила вызывают сомнения, в сделке по российскому праву использование результата дообученной модели, на наш взгляд, возможно в рамках режима правомерного владения экземпляром ПО (в части файла с измененными весами или адаптеров).

Что касается методов неполного (ограниченного) дообучения модели (PEFT), то здесь вопрос возникновения самостоятельного титула на результаты дообучения является еще более спорным, с учетом того, что:

- объемы данных для настройки адаптеров существенно меньше, чем используемые для формата полного дообучения;
- степень модификации модели кратно ниже;
- результат обучения представляет собой файл с дообученными адаптерами, составляющими лишь незначительную часть весов модели, тогда как основная часть не затрагивается.

1.2.5 Адаптация модели без дообучения: титул на данные

Большинство ИИ-систем, используемых компаниями, в том числе выступающими объектами сделок VC и M&A, имеют надстройку RAG. Это **не метод дообучения модели**, в результате создания RAG **параметры модели не изменяются**. При этом RAG существенно обогащает контекст диалогов с моделью, ее ответы становятся более точными, снижаются риски т. н. «галлюцинаций» (ответов, выдуманных моделью, не опирающихся на факты).

RAG-надстройка как актив

Вопрос о том, что такое RAG-система как актив, не имеет однозначного ответа. RAG представляет собой архитектурное решение (технологический конвейер), включающее совокупность программных, модельных и информационных компонентов, и его правовая квалификация во многом зависит от способа интеграции в бизнес-модель компании.

С практической точки зрения способы интеграции RAG в ИИ-систему могут различаться. К ключевым из них относятся:

1. **Закрытая система**	RAG дополняет ИИ-систему исключительно на основе собственной базы знаний владельца.
2. **Партнерская модель**	RAG использует базу знаний одного или нескольких партнеров (например, ИИ-помощник юриста, интегрированный со справочно-правовой системой).
3. **Модель с внешним поиском** (веб-ориентированная)	ИИ-система по запросу пользователя обращается к открытым интернет-источникам и учитывает их при генерации ответа.

4. **Пользовательская модель** (bring your own knowledge)

Система позволяет пользователю загружать собственную базу знаний (документы, инструкции) и учитывает эту информацию при ответе на его запросы.

В рамках одной ИИ-системы указанные конфигурации RAG могут существовать как по отдельности, так и в различных сочетаниях. В ИИ-системе также может использоваться внешний сервис (RAG-as-a-Service), интегрируемый с системой через API.

От выбранной конфигурации напрямую зависит состав активов RAG и их экономическая ценность. В качестве общего перечня можно выделить **следующие активы в составе RAG**:

1. **Программное обеспечение (ПО) чанкинга, векторизации и индексации**

Это комплексное программное решение, которое: (i) разбивает исходный текст на фрагменты (чанки); (ii) преобразует каждый чанк в векторное представление (эмбеддинг) или обеспечивает вызов эмбеддинг-моделей[31] для преобразования текста в векторные представления; (iii) формирует из этих векторов поисковый индекс.

2. **База знаний** (набор данных)

Это «топливо» RAG — исходные документы, тексты, базы ответов, которые система использует для извлечения релевантной информации. Именно база знаний придает RAG содержательную ценность. Такая база может формироваться из собственных, партнерских или пользовательских данных в зависимости от выбранной модели.

3. **Векторное хранилище** (векторная БД)

Векторное хранилище (векторная БД). Это машиночитаемая база данных, в которой сохраняются все созданные эмбеддинги элементов базы знаний.

Эффективность RAG определяется не только качеством входящих в него компонентов, но и организацией оркестрационного слоя ИИ-системы (см. далее подраздел 1.3.). Он отвечает за то, в каком объеме, когда и на основании каких правил система извлекает релевантную информацию для обогащения запроса пользователя.

> **RAG не является методом дообучения базовой модели, в результате создания этой надстройки параметры модели не изменяются. С правовой точки зрения RAG-система — комплексный актив, включающий разнородные объекты, каждый из которых подчиняется собственному правовому режиму.**

В наибольшей степени на эффективность RAG и его практическую ценность влияют база знаний, оркестрационный слой, способы разбиения текста на чанки и настройки поиска.

[31] Эмбеддинг-модели являются самостоятельными ИИ-моделями.

Правовая квалификация RAG

RAG-система

Это комплекс взаимосвязанных технологических компонентов, различающихся как по функциональному назначению, так и по способу создания и использования. Каждый из этих компонентов может иметь самостоятельную экономическую ценность. С правовой точки зрения RAG-система не может быть квалифицирована как единый объект права. Она представляет собой составной (комплексный) актив, включающий разнородные объекты, каждый из которых подчиняется собственному правовому режиму.

#ПРАВОВОЙ_РЕЖИМ

Правовая квалификация ключевых компонентов в составе RAG в обобщенном виде может быть представлена следующим образом:

Программное обеспечение

Программная оболочка RAG-системы охраняется в качестве объекта авторского права (программы для ЭВМ). Данный правовой режим имеет и СУБД, обеспечивающая хранение и управление векторами.

Как отмечалось ранее, ИИ-модели (в данном случае эмбеддинг-модели) также могут рассматриваться как ПО или его часть, однако их правовая квалификация остается дискуссионной.

База знаний (набор данных)

Среди экспертов высказываются различные позиции в отношении режима правовой охраны набора материалов в составе базы знаний. В частности, рассматриваются следующие варианты:

- База данных, охраняемая авторским правом (п. 1 ст. 1260 ГК РФ). В этом случае у ее владельца возникает исключительное право на составительство (расположение и подбор материалов). Такой режим охраняет структуру, а не контент, поэтому этот он мало что дает владельцу такой базы.
- База данных, охраняемая смежным правом ее изготовителя (ст. 1333 ГК РФ). Здесь возникают все те же проблемы, что и описанные выше в отношении более крупных датасетов. При этом число самостоятельных материалов базы знаний для RAG может быть значительно меньше 10 тыс. Поэтому в данном случае доказать существенность затрат, понесенных на создание такой базы данных, будет гораздо сложнее.
- Режим ноу-хау (ст. 1465 ГК РФ) — данный режим является наиболее слабым с точки зрения правовой охраны значимых объектов, поскольку он сильно зависит от фактической способности обеспечить секретность данных, что крайне сложно реализовать на практике, даже при безупречном юридическом оформлении.

Векторная база данных

Данный объект, на первый взгляд, не является охраноспособным, поскольку выступает в качестве технической формы организации базы знаний. Векторная база данных формируется в результате преобразования исходных данных (текста) в эмбеддинги и, таким образом, имеет производный характер по отношению к первичной базе знаний.

Такая база создается посредством математических преобразований при ограниченном участии человека и потенциально спорном творческом вкладе на этапе генерации векторных представлений. Это осложняет ее квалификацию в качестве самостоятельного объекта ИС.

В качестве альтернативы некоторые IT-юристы предлагают квалифицировать эмбеддинги как данные в составе ПО либо рассматривать векторную базу данных в целом как базу данных, охраняемую смежным правом. В рамках более широкого подхода предлагается охрана массива данных такой базы в режиме ноу-хау.

#ПРАВОВОЙ_РЕЖИМ



Роман Головацкий

партнер

Dénuo

Правовая квалификация архитектурного шаблона RAG представляет известную сложность. RAG опирается на базу знаний как на источник данных (наборы документов, инструкции, таблицы и прочее), из которых строится поисковый индекс — данные фрагментируются (разбиваются на чанки (chunks)), преобразуются в числовые векторы (эмбеддинги), которые хранятся в векторной базе данных. В ходе работы система ищет чанки, чьи векторы ближе всего к вектору вопроса, и за счет этого умеет находить смысловые совпадения даже при отличающихся формулировках. В этом смысле векторный (семантический) поиск или же его гибридный вариант выгодно отличаются от классического поиска по ключевым словам.

При квалификации той части системы, которая относится к базе знаний, может быть несколько подходов, но все они не лишены недостатков. Определение ее в качестве охраняемой авторским правом базы данных вряд ли будет справедливым. Авторское право распространяется только на саму структуру базы данных и организацию ее элементов. Однако в базе знаний RAG-системы ключевым является не столько структура как таковая, сколько сами знания, источники данных.

Квалификация базы знаний как ноу-хау, т. е. как некоего набора конфиденциальных сведений, тоже проблематична. Далеко не все сведения, используемые системой в качестве источника данных, могут отвечать требованиям конфиденциальности.

Наиболее близким правовым режимом можно было бы считать смежное право изготовителя базы данных, но только при условии, что такая база содержит не менее 10 тысяч самостоятельных материалов или при наличии других доказательств существенности затрат на ее создание. Между тем в отношении базы знаний RAG-системы это не может быть гарантировано.

В силу вышеуказанных причин, при оценке компонентов RAG неизбежно возникает вопрос наличия титула (т. е.

исключительного права) на базу знаний как на объект интеллектуальной собственности. Представляется, что не во всех случаях этот вопрос может быть разрешим. Другим значимым вопросом является правомерность использования отдельных материалов в составе такой базы знаний.

Что касается программной оболочки RAG-системы (включая модули, отвечающие за векторизацию чанков, управление векторной базой данных, поиск, и т. п.), то, очевидно, что эта часть охраняется авторским правом как программа для ЭВМ.

Отдельную правовую проблему представляет правильная квалификация эмбеддингов, т. е. результатов математического преобразования чанков или других элементов в их векторные представления. Между тем полагаю, что их можно рассматривать как часть программы для ЭВМ в виде машиночитаемых данных, функционально необходимых для работы системы. По своей сути получение эмбеддингов представляет собой технический процесс преобразования данных в рамках кооперации отдельных модулей системы, где один модуль (модуль векторизации) производит такие операции для того, чтобы обеспечивать работу другого модуля системы (retrieval-модуль или модуль семантического поиска).

#ПРАВОВОЙ_РЕЖИМ



Софья Смирнова

советник M&A
и корпоративной практики

O_2 консалтинг

Когда мы структурируем сделку в отношении ИИ-сервиса, первый вопрос — что именно мы покупаем. Большинство коммерческих ИИ-продуктов — это не просто LLM (которая, скорее всего, является программой для ЭВМ в значении ст. 1261 ГК РФ), это RAG-система (архитектура[32], в которой LLM обращается к внешней базе данных для генерации ответа). Возможно утверждать, что это не единый объект IP, это совокупность нескольких объектов с различным правовым режимом.

Так, код пайплайна (функции ингеста, поиска, оркестрации) — программа для ЭВМ. Сами по себе эмбеддинги (числовые массивы (координаты в базе), из которых нельзя[33] восстановить исходный текст) не являются ни произведениями, ни производными произведениями от текста, из которого они созданы; это данные, созданные программой (специальной эмбеддинговой моделью) для функционирования уже другой программы (модуля поиска). С этой точки зрения эмбеддинги являются несамостоятельной частью программы для ЭВМ. Векторная база данных (конкретная совокупность эмбеддингов и метаданных (ссылка на ID документа, временная метка и т. п.), которая позволяет делать полноценный семантический поиск по базе данных (и которая как раз составляет «информационный элемент»), поскольку она создается не творческим подбором, а автоматизированно, может охраняться смежным правом изготовителя, если на ее создание понесены существенные затраты (п. 1 ст. 1334 ГК РФ).

[32] Справочно: RAG-система объединяет несколько компонентов в единый функциональный поток («пайплайн»): (i) Ингест-модуль: программный код, осуществляющий загрузку документов, их разделение на фрагменты (чанки), преобразование в эмбеддинги и запись в векторную базу данных; (ii) Векторная база данных: хранилище эмбеддингов; (iii) Модуль поиска (retrieval): программный код, преобразующий запрос пользователя в эмбеддинг, находящий релевантные фрагменты и передающий их в LLM как дополнение к контексту; (iv) LLM (generation): модель, генерирующая итоговый ответ на основании запроса и найденного контекста; (v) Оркестратор: программный код, координирующий взаимодействие всех компонентов.

[33] Тем не менее восстановление исходных сведений из эмбеддингов технически возможно, по крайней мере частично. В силу этого самим составлением эмбеддингов без согласия правообладателя при определенных сценариях могут считаться нарушенными права на оригинальное произведение. Далее, возникает вопрос о соответствии корпуса эмбеддингов, к примеру, законодательству о персональных данных.

При создании RAG-системы инженер принимает множество нетривиальных решений: какие тексты включить в корпус, как разбить их на чанки (по абзацам, предложениям, с перекрытием или без), какую модель эмбеддингов выбрать, какие метаданные присоединить к каждому вектору, как настроить индексацию. Совокупность этих решений формирует уникальную «карту знаний» — то, как информация структурирована в многомерном пространстве векторной базы данных. Можно ли считать это творческим подбором и расположением? Если да, сама база данных может приобрести статус базы данных, охраняемых авторским правом, а такое инженерное решение может охраняться как ноу-хау. Разные инженеры, работая с одним и тем же исходным корпусом, создадут разные векторные базы.

Стоит отметить, что, поскольку перечень способов использования в ст. 1270 ГК РФ открытый, суд может квалифицировать генерацию эмбеддингов из охраняемого правом произведения как «иное использование»: пока данный вопрос не нашел отражения в судебной практике, возможно распределять риски между сторонами сделки.

С этой точки зрения в договорной документации может быть рискованно ограничиваться all-in формулировкой (например, «все права на Продукт»): желательно раздельно описывать передачу прав на каждый слой: исключительное право на код, смежное право на базу данных, обязательства по конфиденциальности системных промптов, лицензию на LLM от провайдера (и структурировать риски соответственно). Если этого не сделать, при споре покупатель рискует обнаружить, что приобрел оболочку без содержания: код без базы, базу без модели, модель без промптов, которые и делали ИИ-продукт конкурентоспособным.

#АНАЛИЗ_РИСКОВ

При любом сценарии, предполагающем использование базы знаний, важно наличие у разработчика ИИ-системы с RAG **правовых оснований** для использования оригинальных материалов, входящих в базу знаний (если таковые являются охраноспособными объектами). Такие материалы будут как минимум воспроизводиться в ИТ-контуре оператора ИИ-системы, а также при создании эмбеддингов. В отсутствие таких оснований их использование может повлечь правовые риски, связанные с нарушением исключительных прав их обладателей.

Отдельного внимания заслуживает пользовательская модель RAG (bring your own knowledge), в рамках которой пользователь может загружать документы, права на которые могут принадлежать третьим лицам. Более подробно возможные риски в этом случае мы попросили прокомментировать **Шермета Курбанова** (SL LEGAL).

#АНАЛИЗ_РИСКОВ



Шермет Курбанов

соруководитель практики интеллектуальной собственности и цифрового права

SL LEGAL

Пользовательская модель RAG (bring your own knowledge) создает специфический набор правовых рисков, связанных с тем, что владелец ИИ-системы утрачивает прямой контроль над происхождением и правовым статусом загружаемых пользователем данных. В отличие от закрытой или партнерской моделей, где база знаний формируется из материалов с известным правовым титулом, в пользовательской модели владелец ИИ-системы по общему правилу не может проверить правомерность загрузки пользователем каждого конкретного документа.

При этом сам процесс функционирования RAG неизбежно включает воспроизведение исходных материалов — их хранение, чанкинг, векторизацию и последующее использование для генерации ответов.

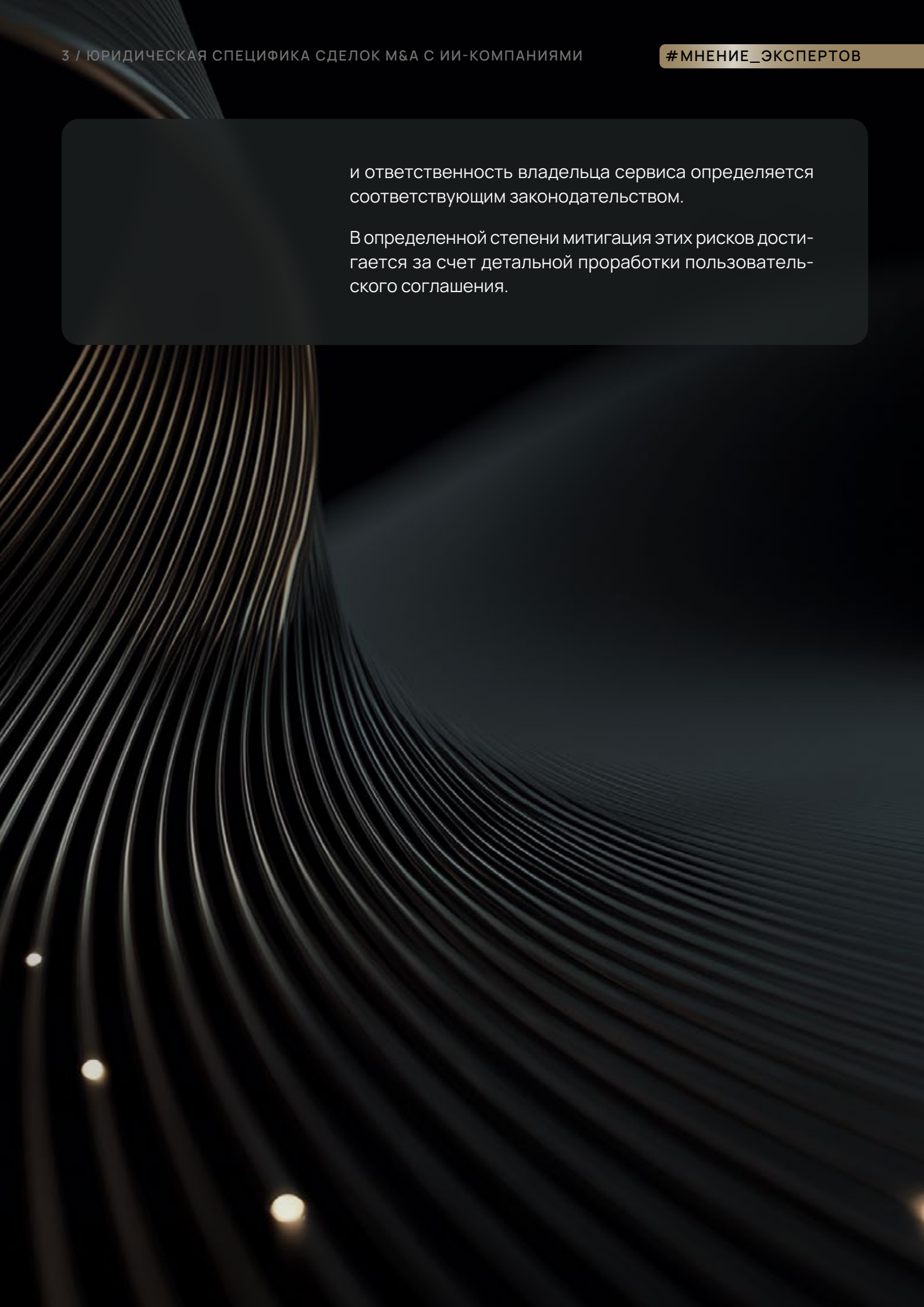
Если пользователь использует ИИ-систему по модели SaaS, при которой вся загружаемая информация размещается на серверах владельца сервиса (стандартная конфигурация для большинства таких систем), и при этом загружает охраняемое произведение без наличия достаточных прав, то владелец сервиса становится лицом, на стороне которого происходит воспроизведение соответствующих объектов.

Само по себе это могло бы квалифицироваться как нарушение исключительных прав. Однако в данном случае к владельцу ИИ-сервиса применим правовой режим информационного посредника (ст. 1253.1 ГК РФ), который при условии добросовестности владельца ИИ-сервиса и своевременного реагирования на уведомления правообладателей (в случае их поступления) позволяет избежать привлечения к ответственности.

Помимо рисков нарушения интеллектуальной собственности, владелец ИИ-системы в пользовательской модели также сталкивается с рисками, связанными с обработкой персональных данных (при загрузке пользователем документов, содержащих ПДн) и материалов с ограниченным доступом. В этих случаях режим информационного посредника не действует,

и ответственность владельца сервиса определяется соответствующим законодательством.

В определенной степени митигация этих рисков достигается за счет детальной проработки пользовательского соглашения.



Вопросы парсинга данных при использовании RAG

Для целей правовой охраны базы знаний RAG наиболее подходящим является режим объекта смежных прав. Поэтому при создании и использовании надстройки RAG также актуален вопрос о рисках, в том числе титульных, связанных с возможным использованием метода парсинга при формировании соответствующей базы знаний. Мы попросили экспертов прокомментировать аспект правомерности парсинга в данном контексте.

#АНАЛИЗ_РИСКОВ



Роман Головацкий

партнер

Dénuo

Значимым вопросом при оценке такого актива, как RAG, является правомерность использования материалов в составе базы знаний.

В закрытых ИИ-системах база знаний RAG может опираться на внутреннюю документацию и материалы. В таком случае следует проверять наличие титула (исключительного права) создателя или оператора ИИ-системы на такие материалы, лицензии или иного правового основания для их использования, если они отвечают критериям охраноспособных объектов интеллектуальной собственности.

Между тем в большинстве случаев RAG опирается на внешние источники данных, и здесь вопрос правомерности их использования представляется более сложным.

Так, использование методов парсинга данных для наполнения базы знаний RAG создает самостоятельный слой правовых рисков на этапе сбора, которые будут далее следовать на всех этапах работы компонентов RAG и в целом ИИ-системы. В частности, такие риски могут сводиться к следующему:

- парсинг может нарушать условия использования того или иного сервиса (например, социальной сети), откуда добываются соответствующие данные автоматизированным способом;
- собираемые материалы могут представлять собой охраняемые объекты интеллектуальной собственности (в частности, объекты авторского права), права на которые принадлежат третьим лицам. Соответственно, без разрешения правообладателей их копирование, сохранение, дальнейшее использование, в том числе выдача фрагментов пользователю через RAG, может считаться незаконным. Следует учитывать, что установленный законом (ст. 1270 ГК РФ) перечень возможных способов использования объектов авторского права, охватываемых исключительным правом, не является исчерпывающим. Соответственно, операции с такими объектами

в RAG-процессах могут быть квалифицированы как «использование» в юридическом смысле и требовать получения согласия от правообладателя;

- в составе собираемых посредством парсинга материалов могут содержаться персональные данные или иная информация с ограниченным доступом. Сбор и дальнейшая обработка таких данных без надлежащего правового основания также будет считаться нарушением и влечь соответствующую ответственность.

Следует отметить, что нахождение парсируемых данных в открытом или условно открытом доступе не означает автоматически возможности их беспрепятственного сбора. Из судебного дела между ООО «Вконтакте» и ООО «Дабл» (А40-18827/2017) можно заключить, что суды могут квалифицировать несанкционированный парсинг социальных сетей как незаконное извлечение материалов из базы данных, охраняемой смежным правом изготовителя.

В контексте нарушения смежного права изготовителя базы данных следует иметь в виду, что закон запрещает:

- перенос всего содержания базы данных или существенной части составляющих ее материалов без разрешения правообладателя (ст. 1334 ГК РФ);
- неоднократное извлечение или использование материалов, составляющих несущественную часть базы данных, если такие действия противоречат нормальному использованию базы данных и ущемляют необоснованным образом законные интересы изготовителя базы данных (ст. 1335.1 ГК РФ).

В этом смысле, как показало указанное дело, суды могут исходить из того, что нарушение установленных правил пользования социальной сетью может входить в противоречие с нормальным использованием соответствующей базы данных и считаться нарушением, даже если из нее извлекается несущественная часть материалов.

#АНАЛИЗ_РИСКОВ



Софья Смирнова

советник M&A
и корпоративной практики

O_2 консалтинг

Создание RAG-системы на основе скрапированных публичных данных — не безусловно допустимая практика. Дело «Дабл Дата» показало, что суды готовы признать нарушением систематический автоматизированный сбор данных с крупной платформы, даже если данные формально открыты для сбора. Три фактора определяют уровень риска: a) является ли источник охраняемой базой данных; b) каков объем и систематичность извлечения; c) содержат ли данные персональные данные.

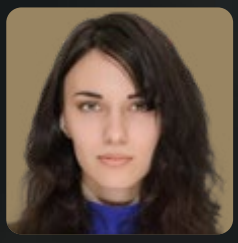
Если ИИ-сервис парсит крупную платформу (соцсеть, маркетплейс), она, скорее всего, защищена как база данных (смежным правом). Копирование ее контента в RAG-систему — это извлечение частей чужой базы. При этом чем больше и систематичнее сбор, тем выше риск.

Далее, если в скрапированных текстах есть персональные данные, эмбеддинги наследуют их правовой режим. Эмбеддинг — это не анонимизация: из него можно восстановить исходный текст, а Роскомнадзор не признает создание эмбеддингов[34] методом обезличивания. Согласие субъекта должно покрывать не только хранение текста, но и его преобразование в эмбеддинг и хранение в векторной базе данных.

Снизить возможные риски создателям ИИ-сервисов на базе RAG со скрапингом поможет следующее: не обходить технические барьеры площадок в Интернете, не извлекать существенную часть, избегать платформ с персданными (без получения соответствующих разрешений), рассмотреть хранение только эмбеддингов без чанков, шифровать векторы, документировать затраты для обоснования собственного смежного права.

[34] Если эмбеддинг снабжен метаданными и хранится вместе с ними, он косвенно определяет субъекта ПДн, что накладывает ограничения на хранение эмбеддингов отдельно от остальных данных. При этом даже без метаданных атака инверсии теоретически способна на восстановление данных субъекта ПДн и из самого вектора, что усложняет соблюдение регуляторных требований, к примеру, по защите от утечек.

#РАСПРЕДЕЛЕНИЕ_РИСКОВ_В_M&A



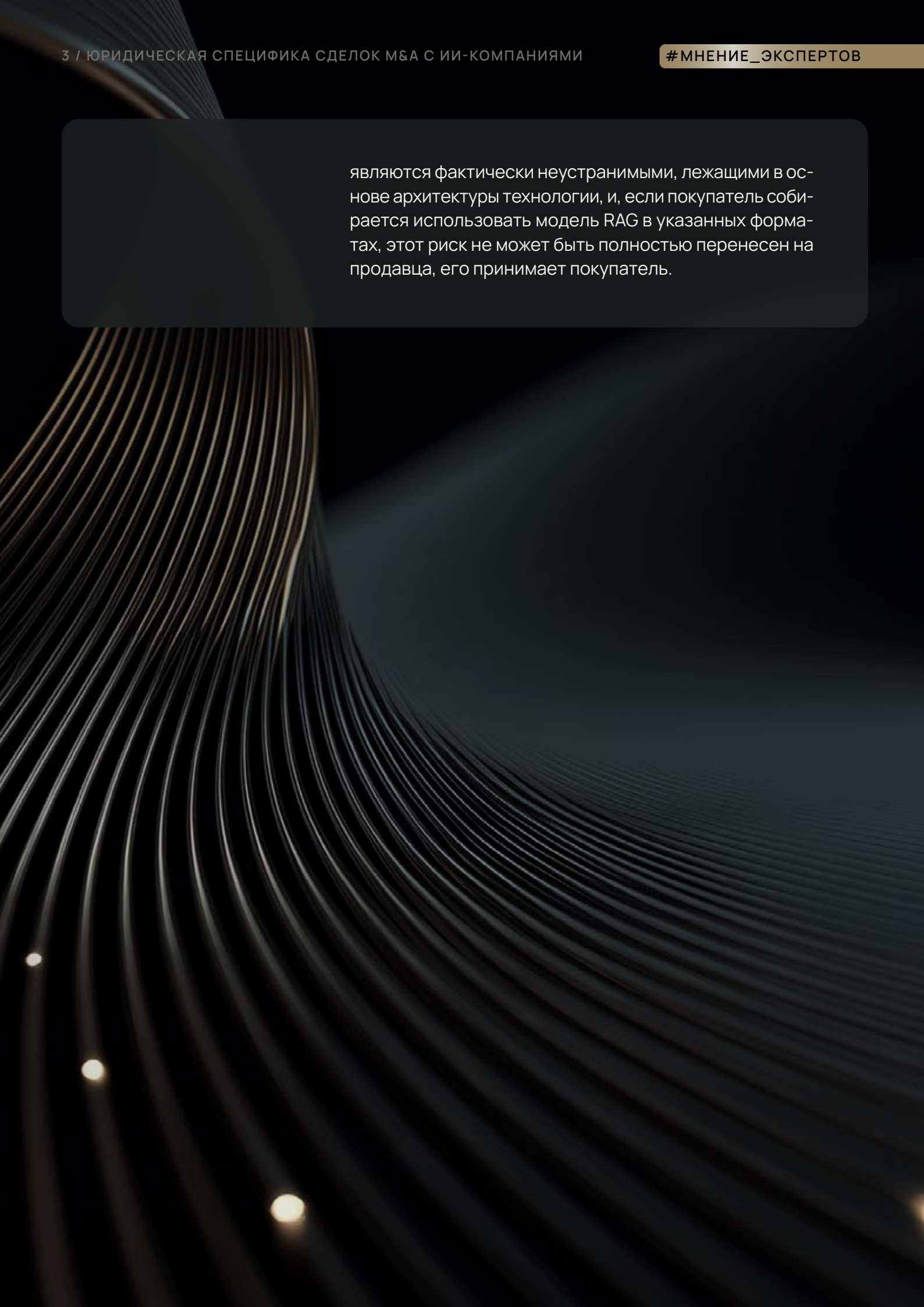
Анастасия Нерчинская

Если слой RAG находится полностью под контролем разработчика ИИ-системы, риски «наследования» эмбеддингами охраняемых данных или интеллектуальной собственности третьих лиц (вне зависимости от того, по какой причине такие объекты попали в исходную человекочитаемую базу материалов, векторизованную для целей RAG) лежат полностью на продавце. К таким случаям относятся большинство форматов RAG со своей базой знаний, вне зависимости от динамики ее обновления, так как источник данных является управляемым. С определенными оговорками сюда относятся и вариант RAG, использующий партнерские базы знаний, поскольку разработчик системы контролирует выбор партнера, а в ряде случаев может на уровне договорных инструментов требовать обеспечения «чистоты» данных партнерской базы, используемых для целей своего RAG.

В первом случае покупатель может запрашивать у продавца бизнеса полные гарантии об отсутствии в системе RAG неавторизованных данных и контента третьих лиц, а также о том, что данные, используемые для целей RAG, не были получены методом парсинга. Во втором допустимы оговорки о «знании продавца» или сужение объема гарантий. Вместо факта юридической «чистоты» в части партнерских данных продавец может настаивать на формулировке «разумных усилий» / «принятии всех разумных мер» для проверки и обеспечения чистоты партнерских данных в целях создания и функционирования RAG-надстройки.

Что касается форматов RAG, в рамках которых используется веб-ориентированная или пользовательская модель, здесь более уместно проводить параллель с ответственностью продавца за аналогичные риски, «наследуемые» от базовой модели. В этом случае подход будет принципиально иным, поскольку в абсолютном большинстве случаев создатель ИИ-системы не имеет разумных возможностей для контроля таких рисков. Он не может проверить авторизацию всех данных, попадающих в RAG из Интернета. Поэтому такие риски

являются фактически неустранимыми, лежащими в основе архитектуры технологии, и, если покупатель собирается использовать модель RAG в указанных форматах, этот риск не может быть полностью перенесен на продавца, его принимает покупатель.



1.2.6 Тренд на ужесточение требований локализации данных

На фоне развития тренда на локализацию и русификацию ИИ все большее значение будет иметь вопрос о том, где формируются, хранятся и используются массивы данных, используемые при создании ИИ-систем, и насколько они адаптированы к регуляторным требованиям и отраслевым сценариям. Для части сегментов рынка это может означать появление дополнительной премии к оценке тех ИИ-активов, которые используют локальные датасеты, обеспечивают обработку данных в российском контуре и способны подтвердить их происхождение и качество.

> **Системные промпты имеют более высокий приоритет для ИИ-модели по сравнению с пользовательскими промптами, а также являются одним из инструментов управления этическими и ИБ-рисками.**

Этот тренд сегодня в общем виде формируется из совокупности различных регуляций.

1. Это требования по **локализации баз данных**, с помощью которых осуществляется сбор персональных данных граждан России. В массивах данных зачастую присутствуют персональные данные, поэтому данное требование напрямую затрагивает разработчиков ИИ-систем.
2. Это вопросы **локализации программного обеспечения**. Например, если программное обеспечение используется на объектах КИИ, оно должно быть включено в РРПО. Включение в такой реестр возможно только при условии, что его разработчик является российской компанией, которая контролируется гражданами России. Это может приводить к косвенной локализации, когда для получения доступа к определенным клиентам необходимо обеспечить разработку в России. Фактически это означает, что и массивы данных будет необходимо накапливать и использовать с применением вычислительных мощностей, расположенных в России.

Наконец, развитием данного тренда являются положения Законопроекта Минцифры, допускающего использование в определенных сферах только доверенных ИИ-моделей. Режим таких моделей предполагает обработку данных исключительно на территории России. Это означает, что данные должны быть в той или иной степени локализованы.

#ТРЕНДЫ



Софья Смирнова

советник M&A
и корпоративной практики

O2 консалтинг

Тенденции законодательного регулирования тяготеют к тому, что рынок будет принадлежать только доверенным ИИ-продуктам, LLM в составе которых прошли специальную сертификацию ФСТЭК и ФСБ. Несмотря на отсутствие прямых ограничений для B2B-использования, B2G и B2C-рынок будет локализовываться, о чем свидетельствует проект ФЗ об ИИ, сформированный Минцифры. Отдельным вопросом является применение к ИИ-сервисам «закона Яровой». Представляется, что в настоящий момент он может быть неприменим, но п. 10.3 проекта ФЗ об ИИ[35] будет применять его к ИИ-сервисам с количеством пользователей более 500 тыс. в сутки.

[35] Законопроект Минцифры (см. определение в Приложении 1).

1.3 Слой оркестрации: ключевые активы

Слой оркестрации является неотъемлемой частью ИИ-системы и предназначен для организации работы и управления всеми компонентами системы при обработке запроса пользователя. Оркестрация определяет, какие данные получает ИИ-модель, к каким инструментам и сервисам обращается, как осуществляет работу и как формирует итоговый результат. Иными словами, это логика, которая связывает все компоненты ИИ-системы в единый рабочий процесс.

#ПРАВОВОЙ_РЕЖИМ

Ключевые активы этого слоя можно разделить на **программные и информационные**.

Правовая квалификация **программных активов** не вызывает сложностей. Это ПО или его части, охраняемые в режиме авторского права. К такому ПО относятся оркестраторы процессов, интеграционные модули и прочие программные компоненты. Обычно такие активы представлены специализированным (инструментарным) ПО и сами по себе не имеют большой ценности. Программный слой может быть проприетарным либо создаваться на основе открытого ПО, что встречается гораздо чаще. В ходе проверки таких активов необходимо устанавливать либо наличие титула (исключительного права), либо иных правовых оснований использования ПО оркестрационного слоя ИИ-системы.

Информационные компоненты данного слоя являются, главным образом, частью оркестрационного ПО, а именно — данными, необходимыми для его функционирования. При этом отдельного внимания заслуживают **системные промпты**, поскольку их правовая квалификация является неоднозначной.

Системные промпты являются одним из важных механизмов управления поведением ИИ-модели. По сути это базовые правила или управляющие инструкции, обеспечивающие стабильную работу ИИ-модели, снижение вероятности некорректных ответов и их необходимую специализацию. Системные промпты имеют более высокий приоритет для модели по сравнению с пользовательскими промптами и являются одним из важных инструментов управления этическими и ИБ-рисками.

Обычно в оркестрационном слое **не хранится какой-то единичный системный промпт**. Оркестратор управляет наборами шаблонов, предназначенных для решения разных задач, собирает системные промпты из разных блоков, использует их различные версии, параметризирует их. Такие наборы компонентов для сборки системных промптов составляют **библиотеки системных промптов**. При этом, в зависимости от задач и сценариев, оркестрационный слой может содержать или подключать несколько таких библиотек. Поэтому часто процесс оркестрации при работе ИИ-системы выглядит как многослойная схема.

#ПРАВОВОЙ_РЕЖИМ

С точки зрения **правовой квалификации** отдельно взятый системный промпт, если он является результатом творческого труда человека, может являться охраноспособным объектом авторского права. Чаще всего он собирается оркестратором из различных компонентов, извлекаемых из библиотек системных промптов, и является функциональной частью ПО оркестрационного слоя.

Как актив ключевое значение имеет именно **библиотека системных промптов**, а не единичные системные промпты. Среди экспертов высказываются различные мнения о возможном правовом режиме охраны библиотек системных промптов. В частности, они могут охраняться как:

- **База данных, охраняемая авторским правом** (п. 2 ст. 1260 ГК РФ). Как упоминалось выше, такой правовой режим охраняет структуру базы данных, а не ее содержимое. В то же время библиотеки системных промптов могут являться организованными структурами данных, основная ценность которых заключается не столько в наборе шаблонов, сколько в том, как они упорядочены и управляются. В последнем случае правовой режим авторско-правовой базы данных вполне подходит.
- **База данных, охраняемая смежным правом ее изготовителя** (ст. 1333 ГК РФ). В части данной квалификации возникают те же проблемы, что и описанные выше в отношении базы знаний для RAG. Число самостоятельных материалов библиотеки системных промптов может быть значительно меньше, чем 10 тыс. Поэтому в данном случае доказать существенность затрат, понесенных на ее создание, сложнее, чем для крупного массива данных.
- **Ноу-хау** (ст. 1465 ГК РФ) — как упоминалось ранее, данный режим является наиболее слабым с точки зрения правовой охраны, поскольку он сильно зависит от фактической способности

обеспечить секретность данных. Однако если библиотеки системных промптов не являются общедоступными, их неизвестность широкому кругу лиц создает коммерческую ценность для их обладателя, то такой правовой режим также может быть использован.

Таким образом, в рамках проверки активов, относящихся к оркестрационному слою, имеет значение наличие правовых оснований не только для использования ПО оркестратора, но и системных промптов, в особенности — библиотек системных промптов, которые использует оркестрационный слой.

Кроме того, некоторые эксперты отмечают, что технические решения, относящиеся к оркестрационному слою ИИ-систем, могут быть также объектами патентных прав (например, способы оркестрации и управления ИИ-моделями).

Мы попросили экспертов рассказать о возможных режимах правовой квалификации активов оркестрационного слоя.

#ПРАВОВОЙ_РЕЖИМ



Софья Смирнова

советник M&A
и корпоративной практики

O_2 консалтинг

Правовая природа системных промптов и библиотек системных промптов внутри ИИ-сервиса на базе RAG-системы не является единой. Возможно несколько подходов: ноу-хау, режим произведения или несамостоятельная часть программы для ЭВМ (если он находится внутри исходного кода). Представляется, что следует использовать все возможные доступные способы защиты (и, соответственно, документировать промпты как отдельный объект передачи в сделке).

Библиотеки промптов могут охраняться авторским или смежным правом на базы данных (в зависимости от наличия творческого подбора библиотеки со стороны инженеров данных). Представляется, что библиотеки промптов должны охраняться скорее как объекты именно авторского права (в силу специфичности их функции и необходимости непосредственного участия инженеров).

#ПРАВОВОЙ_РЕЖИМ



Роман Головацкий

партнер

Dénuo

Вопрос правовой квалификации оркестрационного слоя ИИ-системы не является тривиальным. Поскольку в первую очередь это программная оболочка, то ближайший и ключевой правовой режим — это охраняемая авторским правом программа для ЭВМ (см. ст. 1261 ГК РФ). Соответственно, с точки зрения оценки чистоты прав его нужно главным образом проверять именно в этом качестве.

В то же время следует учитывать, что отдельные решения в области оркестрации ИИ-систем могут быть предметом патентной охраны. Так, например, в США могут патентоваться относящиеся к оркестрационному слою системы и способы обеспечения миграции между различными ИИ-платформами (*US20210390426A1 — Artificial intelligence orchestration layer to facilitate migrations between different artificial intelligence platforms*), системы и способы определения ограничений для ИИ-

агентов и их рабочих данных, мониторинга и оценки их поведения (*US20260017525A1 — Validating autonomous artificial intelligence (AI) agents using generative ai*), системы и способы, управляющие с помощью оркестратора множеством ИИ-агентов для генерации ответа на входные данные (*US12111859B2 — Enterprise generative artificial intelligence architecture*). Патентоваться могут также специфические для отдельных индустрий решения. Например, системы и способы интегрированной оркестрации когнитивными сервисами, такими как обработка естественного языка, анализ настроений, распознавание речи, преобразование текста в речь и компьютерное зрение (*US20220116485A1 — Integrated orchestration of intelligent systems*). Для Российской Федерации получение патентной охраны на такие решения может быть сложнее в силу имеющихся методологических ограничений (жесткая привязка патентуемого решения к техническому результату). Однако, учитывая существующий в настоящее время в РФ тренд на либерализацию подходов в области патентования IT-решений, возможности получения такой охраны в дальнейшем также будут расширяться.

Отдельного упоминания заслуживают такие элементы слоя оркестрации, как системные промпты и библиотеки системных промптов. Причем хотя некоторые творческие промпты и могут быть охраноспособными (в режиме авторского права — ст. 1259 ГК РФ), большее значение в качестве актива имеют именно библиотеки. Это связано с тем, что в большинстве случаев системные промпты формируются и генерируются самим оркестрационным слоем из шаблонов, модулей и иных компонентов библиотек системных промптов.

Библиотека системных промптов может охраняться в рамках правового режима авторского права в качестве базы данных (п. 2 ст. 1260 ГК РФ). Этот режим релевантен, если ценность библиотеки заключается не только в содержащихся в ней компонентах, но и в самой организации структуры данных. С точки зрения правовой охраны непосредственно данных здесь может быть релевантен режим ноу-хау, при условии обе-

спечения конфиденциальности данных библиотеки (ст. 1465 ГК РФ). Также стоит отметить и режим смежного права изготовителя базы данных (ст. 1334 ГК РФ), но он труднодостижим, поскольку для библиотеки системных промптов может быть проблематично доказать существенность затрат, которая требуется для возникновения охраняемого права.



Анатолий Земцов

управляющий партнер

dfcenter

С технической точки зрения важно различать программный слой оркестрации (код, управляющий вызовами модели, маршрутизацией запросов и интеграцией с внешними API) и конфигурационные артефакты, определяющие поведение модели внутри этого слоя.

Ключевым активом среди таких артефактов являются системные промпты и их библиотеки. В архитектуре современных агентных систем они выполняют функцию, аналогичную «программированию на естественном языке»: задают ролевую модель, границы допустимого поведения, формат ответа и бизнес-логику взаимодействия.

Качественный системный промпт, отлаженный для промышленной эксплуатации, является результатом значительных инженерных усилий и обладает самостоятельной коммерческой ценностью.

При этом ценность создается не самим фактом наличия промптов, а их способностью стабильно и предсказуемо направлять поведение модели в рамках программно-детерминированного контура оркестрации (Router-based architecture). Именно сочетание жесткой программной логики и гибких инструкций на естественном языке обеспечивает баланс между управляемостью и адаптивностью системы.

Раздел 2

Due diligence и ключевые риски ИИ-бизнесов

АВТОРЫ



Анастасия Нерчинская



Роман Головацкий
DENUO



Александр Панов
VERBA LEGAL



Анатолий Земцов
DFCenter

Краткие выводы

- Основные юридические риски, связанные с созданием и функционированием ИИ-систем, лежат в плоскости данных. К ним относятся риски, связанные с: (i) нарушением прав на чужие ОИС; (ii) обработкой ПДн без надлежащих правовых оснований; (iii) неправомерным распространением, получением или использованием информации ограниченного доступа; (iv) оспариванием титула на датасеты, сформированные методом парсинга; (v) невозможностью эксплуатации ИИ-систем, неправомерно использующих данные.

- Многие из рисков ИИ-системы являются регуляторными и могут повлечь крупные денежные штрафы. В отношении ИИ-активов они могут существенно мультиплицироваться с учетом объема используемых данных. Архитектурные свойства ИИ-технологии не позволяют удалить из модели отдельные проблемные фрагменты. Исполнить решение суда о прекращении использования спорных объектов (например, неправомерно обрабатываемых ПДн) можно только путем удаления всей модели или ее «дообученной» части, если таковая локализована (например, отдельные «дообученные» адаптеры).

- Частноправовые риски, связанные с использованием неавторизованных ОИС, также могут повлечь существенные денежные штрафы / компенсации, либо запрет на их использование при эксплуатации ИИ-системы. Однако, в силу тех же архитектурных свойств ИИ, какие-либо объекты, «хранящиеся» в модели, в том числе, представленные в векторном формате, не могут быть исключены из нее иначе, как путем удаления всей модели. Фактически, это будет означать прекращение бизнеса либо его длительную приостановку, требующую дорогостоящего перезапуска.



Илья Булгаков
DENUO



Шермет Курбанов
SL Legal

- Аналогичные частноправовые риски могут возникать и в отношении информации с ограниченным доступом (например, охраняемой в режиме коммерческой тайны). Это касается также тех ситуаций, когда доступ к такой информации получен случайно или по ошибке. В последнем случае обладатель информации может потребовать обеспечить конфиденциальность даже в отсутствие заключенного NDA, и несоблюдение такого требования может повлечь обязанность возместить убытки, размер которых при их доказанности может оказаться значительным.

- И регуляторные, и частноправовые, включая титульные, риски, потенциально устранимы (в том числе путем удаления локализованной дообученной модели) только в том случае, если они относятся к данным или иным слоям системы, контролируемым ее оператором. Если такие риски выявлены только применительно к предобучающим данным и модели, которые не контролирует оператор системы, — фактически они являются неустранимыми.

- Неустранимые риски ИИ-системы сосредоточены в основном на уровне предобучающих датасетов и базовой модели. Они не подлежат юридическому, а также, в большинстве случаев, техническому анализу, поскольку являются закрытыми для прямого доступа третьих лиц. Этот вопрос атрибутируется разработчику модели, который не является стороной сделки. Соответственно, оператор системы не может обеспечить экспертизу предобучающих датасетов.

- Фокус юридического due diligence ИИ-системы сосредоточен в слоях: (i) модели (преимущественно на уровне полномочий по ее использованию и результата ее адаптации); (ii) данных (в части, контролируемой оператором системы, включая дообучение, RAG-надстройки); (iii) оркестрации (включая библиотеки системных промптов); (iv) инфраструктуры; (v) политик и процедур по управлению жизненным циклом ИИ-системы.

- С учетом развития тренда на локализацию данных, используемых для целей обучения ИИ, а также русификацию ИИ-моделей, ожидаемо появится новый тип ИИ-рисков, связанных с возможным отсутствием подтверждения (в том числе путем сертификации) национального происхождения моделей.

- В 2025 г. в рамках создания ИИ-решений часто использовались зарубежные модели. Транснациональный характер большинства базовых моделей и датасетов существенно осложняет анализ ИИ-систем, созданных на их основе, и нередко требует привлечения специалистов по иностранном праву. Также к типовым трудностям анализа ИИ-систем можно отнести большие объемы датасетов, что делает экстраполяцию выводов, сделанных на основе небольшой выборки, соразмерной адекватному ресурсу для ее проверки, неточной.

- Одной из особенностей юридической проверки ИИ-системы является высокая значимость проведения покупателем технической экспертизы. Если к соответствующим ИИ-артефактам есть прямой доступ, желателен формат экспертизы white-box, позволяющий изучить «внутреннее устройство» объекта. Минимальным стандартом осмотрительности покупателя будет являться формат проверки black-box, позволяющий по косвенным признакам понять особенности поведения ИИ-актива или его конкретных артефактов без прямого доступа к «начинке».

- Ключевой особенностью ИИ-бизнеса является то, что основные юридические риски являются заведомо высокими, несмотря на то, что многие из них, на первый взгляд, представляются гипотетическими и сложно детектируемыми. Это связано с: (i) крайней технологической сложностью обеспечения «чистоты» обучающих датасетов; (ii) заведомо высокой степенью мультипликации рисков в силу огромного объема используемых данных; (iii) очень высокой стоимостью митигации рисков, сопоставимой со стоимостью бизнеса или превышающей ее.

- Помимо юридических, бизнес ИИ-компаний сопряжен с иными типами рисков, в первую очередь, этическими (алгоритмическая дискриминация модели, необъяснимость ее ответов и ряд других), техническими (в частности, дрифт концепции, данных и модели), ИБ-рисками (например, промпт-инъекции, риски утечек). Их анализ при приобретении ИИ-компании также очень важен, он проводится силами многопрофильной команды экспертов из соответствующих областей.

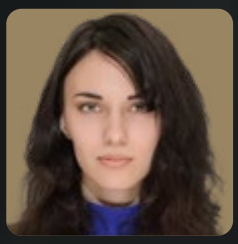
Эксплуатация ИИ-систем может порождать различные риски информационного, этического, технического, регуляторного и юридического характера, включая риски причинения вреда пользователям в связи с различного рода инцидентами. Конкретные типы рисков напрямую зависят от индустрии бизнеса, сферы использования и целей применения ИИ-системы, а также масштаба деятельности, в основе которой лежит ИИ-технология. Не вызывает сомнений, что сложные мультиагентные системы, степень поведенческой автономности которых кратно выше, чем, например, у класса решений-«ассистентов», будут иметь гораздо более высокий риск-профиль, и при приобретении соответствующего бизнеса требования к их проверке ожидаемо будут более высокими.

Юридический due diligence ИИ-активов **существенно отличается от анализа традиционных программных продуктов**. Подходы к юридической проверке необходимо адаптировать для целей анализа ИИ-систем, иначе она не будет эффективной и окажется очередной формальностью. В процессе due diligence ИИ-системы возникают все те же сложности, что и при проверке «обычного» ПО, поскольку ИИ-система — это программный комплекс, в котором помимо ИИ-компоненты всегда присутствует традиционный ИТ-стек без ИИ в своей основе. ИИ-система, также как и любое сложное ПО, — многослойный и многокомпонентный объект, «невидимый» для обычного человека, не владеющего экспертизой программирования, динамичный и постоянно обновляемый, крайне сложно идентифицируемый и фиксируемый «на бумаге», включая цели его описания в конкретный момент времени. ИИ-система также создается и поддерживается множеством разработчиков, многие из которых являются соавторами различных его частей. Все эти аспекты существенно осложняют юридический due diligence даже традиционных программных продуктов или ИТ-систем, которые не связаны с ИИ-технологией.

Однако проверка ИИ-активов **принципиально осложняется** тем, что логика поведения ИИ-компонента, в отличие от традиционного ПО, **недетерминирована** в силу архитектурных свойств технологии — стохастичности и вероятностного характера результатов ее работы (ответов ИИ-модели). С этим связана центральная сложность ИИ-технологий — **проблема атрибуции инцидентов и дефектов поведения и ответственности за них в разрезе «модель-система»**. Именно она нашла отражение во всех областях ИИ-рисков, включая этические, технические и юридические.

В рамках данного исследования мы провели множество интервью с ИИ-экспертами, включая тех, кто сопровождает сделки Tech M&A с ИИ-активами, которым адресовали ряд наиболее сложных вопросов, связанных с проверкой юридических рисков[36] при приобретении бизнеса, функционирующего на основе ИИ-систем. Многие вопросы, связанные с рисками ИИ-бизнесов и подходами к их распределению между сторонами сделки, мы рассмотрели в предыдущем разделе исследования. В этом разделе анализ рисков ИИ-активов основан на итогах проведенного опроса и обзоре экспертных комментариев.

[36] При этом важно отметить, что иные категории рисков (этические, технические, риски, связанные с информационной безопасностью) не менее важны для анализа, чем юридические.



Анастасия Нерчинская

В любом продукте, в основе которого лежит ИИ-технология, всегда есть риски, многие из которых:

1. **Принципиально недетектируемы**. Их либо невозможно выявить и проанализировать вообще (ни обычными, ни зачастую специализированными методами), либо без несоразмерных затрат на этот процесс. Например, в абсолютном большинстве случаев в рамках юридического due diligence невозможно проверить «чистоту» предобучающего датасета базовой модели, а если модель несколько раз переобучалась / дообучалась — то и соответствующих датасетов тоже, за исключением случаев, когда такое дообучение проводилось самим разработчиком системы или под его контролем.
2. **Проверяемы, но на них невозможно повлиять**. Их можно либо принять, либо отказаться от модели. Например, можно (и нужно) тщательно проверить условия использования базовой модели. Во многих случаях — это открытая информация, доступ к которой есть у любого лица, включая гипотетического покупателя соответствующего ИИ-бизнеса. Однако если покупатель на этом уровне обнаружит риски, препятствующие использованию ИИ-решения, использующего такую модель, например, в силу ограничений по количеству конечных пользователей модели или сферам ее монетизации, — он вряд ли может пойти к разработчику модели и «передоговориться» об условиях. Модели распространяются на основании условий, к которым пользователь зачастую лишь присоединяется, но не может влиять на их содержание. Поэтому на этапе due diligence важно попытаться понять все доступные опции бесшовной с технической и юридической точек зрения замены модели на другую.
3. **Непереносимы на контрагента (продавца бизнеса) в принципе**. Продавец, владеющий компанией-оператором ИИ-системы, не является их носителем (также как и непосредственно сам оператор системы), — не он создавал ИИ-технологию и опре-

делял ее архитектурные свойства. В частности, продавец принципиально не может отвечать за абсолютное множество возможных дефектов, связанных с обучением базовой модели, и слой предобучающих данных, если, конечно, он сам не является разработчиком модели или, в некоторых случаях, поставщиком данных для ее обучения.

4. **Носят вероятностный (неточный) характер**. Даже те риски, которые потенциально полноценно проверяемы в силу того, что объект проверки контролируется оператором системы (например, приобретенный или созданный своими силами крупный дообучающий датасет), — не могут быть проверены с высокой точностью. Технически white-box экспертиза может существенно помочь выявить проблемные области в тех объектах, к которым у оператора системы есть прямой доступ (например, свой датасет). Но многие методы проверки основаны на анализе выборки, а не всей совокупности элементов объекта. В силу того, что крупные датасеты огромны (даже дообучающие, которые, в сравнении с предобучающими — малы, но для целей экспертизы — очень велики), — часто применяется метод выборки с последующей экстраполяцией выводов. Особенно это касается юридической проверки. Например, выборка, сформированная для целей проверки получения правовых оснований использования различных категорий данных из огромного массива данных, будет заведомо крайне мала. А при экстраполяции выводов вероятность ошибок в оставшейся части элементов — всегда будет очень велика. Поэтому ИИ-технология считается высокорисковой при любой степени проверки.
5. **Не устранимы или устранимы радикальными способами**. Если покупатель обнаружит риски (в том числе с применением методов black-box тестирования) на уровне обучающих данных базовой модели — оператор системы (таргет или продавец) не сможет просто так (например, в рамках выполнения отлагательных условий закрытия) пойти к разработчику модели и заставить его удалить модель

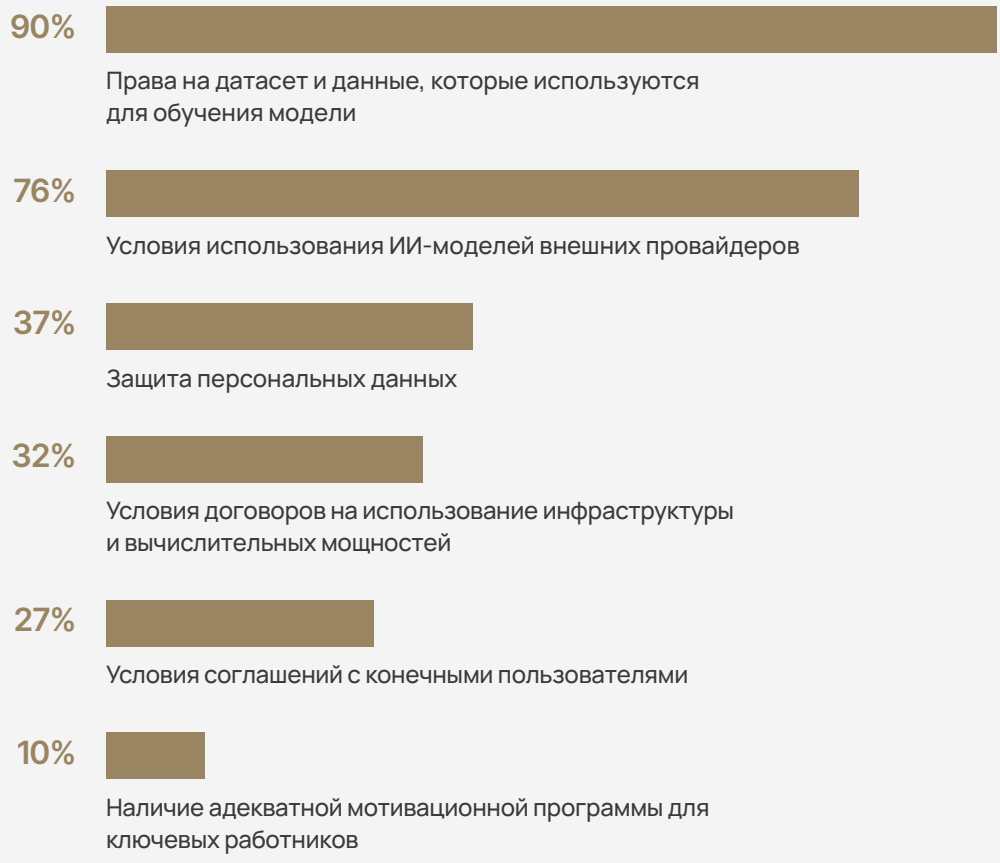
с дефектами или переобучить ее. Если упрощенно, он лишь может попросить оператора системы заменить модель, но при этом полностью принять исторические риски прежней, «дефектной» модели. Однако если такая проблема будет обнаружена в датасетах, контролируемых самим разработчиком системы, — ее оператор уже не сможет ссылаться на модель. Риски этого слоя — его зона ответственности, поэтому ему придется выбирать между заменой модели или ее переобучением на тех же, но уже «вылеченных» данных, но при этом — полностью отвечать за соответствующие исторические риски, если после закрытия сделки компании будут предъявлены претензии.

2.1 Приоритетные области юридической проверки ИИ-активов

В рамках проведения исследования был проведен онлайн-опрос об областях юридической проверки при приобретении ИИ-компаний, на которых респонденты фокусировались в первую очередь. Ответы участников опроса приведены на графике ниже.

#РЕЗУЛЬТАТЫ_ОПРОСОВ

Приоритетные области юридической проверки ИИ-компании



По данным Опроса по аспектам Tech M&A (41 респондент).

Мы попросили ИТ-экспертов прокомментировать результаты опроса и рассказать о своем опыте юридической проверки ИИ-бизнесов.



Роман Головацкий

партнер

DÉNUO

Результаты опроса показывают, что самыми приоритетными областями для юридической проверки являются права на датасет и обучающие данные, а также условия использования ИИ-моделей. Это неудивительно, поскольку данные области критичны для бизнеса, основанного на ИИ-решениях.

Данные — это «кровь» ИИ-системы, то, без чего бизнес функционировать не может. Они определяют поведение модели, формируют конкурентные преимущества продукта, его уникальность и безопасность. Но одновременно это и высокая область материализации юридических рисков, вытекающих из оснований использования данных.

Важность условий использования модели обуславливается тем, что большинство ИИ-систем опираются на сторонние ИИ-модели и перманентно зависят от них. Поэтому оценка пределов и ограничений использования модели необходима для подтверждения правомерности функционирования бизнеса в его текущем формате, его масштабируемости, устойчивости, а также соответствия задачам покупателя.



Анна Максименко

партнер

KKMP LEGAL

В юридической проверке ИИ-активов необходимо сфокусироваться на следующих аспектах:

1. **Права на ИИ-модель**: какая ИИ-модель используется (иностранное или российское решение), кто его поддерживает и какие источники данных используются для обучения. ИИ-модель — это не один объект, а связка обучающих данных, алгоритмов, кода и инфраструктуры. Ошибки на этапе создания ИИ-модели, такие как обучение на незаконно полученных данных, нарушение прав правообладателей или субъектов персональных данных, могут привести к требованиям уничтожить не только данные, но и саму модель, как это уже происходило в зарубежной практике.
2. **Работа ИИ с данными**: насколько работа ИИ с различными категориями поступающих в нее данных, среди которых могут быть персональные данные и иная информация, подлежащая защите, соответствует требованиям применимого законодательства.
3. **ИИ комплаенс**: какие решения принимает ИИ, являются ли они обязательными, как выстроен человеческий контроль, нет ли дискриминации и нарушений трудового, антимонопольного и отраслевого регулирования.
4. **Права на результаты генераций ИИ**: какие результаты генерирует ИИ и какие права на результаты генераций есть у приобретаемой компании. Результаты, созданные с помощью ИИ (например, программный код, изображения, контент, произведения), могут представлять собой ключевую интеллектуальную собственность приобретаемой компании.



Шермет Курбанов

соруководитель практики интеллектуальной собственности и цифрового права

sll
SL LEGAL

Конкретные области и глубина необходимого анализа зависят от типа ИИ-таргета, структуры сделки, способов использования ИИ-активов и сегмента (отрасли) бизнеса компании.

Ключевые направления юридической и технической экспертизы (в дополнение к традиционным) включают:

- Вопросы интеллектуальной собственности с акцентом на обучающий датасет и использование в ИИ-активе IP третьих лиц, их влияние на ИИ-активы таргета и требования к ним.
- Отраслевые аспекты (например, банки, медицина) и регуляторные требования (в т. ч. объекты КИИ, контрсанкционный комплаенс) к бизнесу.
- Вопросы персональных данных с акцентом на обучающий датасет и обработку в ИИ-активе персональных данных третьих лиц.
- Договоры с ключевыми поставщиками ИИ-сервисов или инфраструктуры и конечными пользователями.
- Аспекты кибербезопасности и защиты от утечек.
- Наличие и достаточность инфраструктуры для текущей и планируемой деятельности, наличие и достаточность компетентного персонала, качество ответов и общая эффективность актива.
- Этические вопросы: предвзятость / дискриминацию (bias), галлюцинации (недостоверная информация при выдаче генераций) и необъяснимость генераций (explainability), выдачу нежелательного или запрещенного контента.

Сложность рассматриваемых вопросов, а также пересечение правовых, коммерческих и технических аспектов требуют комплексного подхода к организации проверки ИИ-бизнеса с участием специалистов из разных областей. Особое внимание следует уделить техническому аудиту ИИ-актива (например, black-box или white-box проверке), поскольку именно технические эксперты предоставляют ключевую информацию, лежащую в основе последующего юридического и бизнес-анализа.



Софья Смирнова

советник M&A
и корпоративной практики

O_2 консалтинг

К ключевым рискам, которые необходимо проверить в рамках due diligence ИИ-бизнеса, мы бы отнесли следующие:

- Защита от предвзятого (несправедливого) или неточного контента в результатах генерации. Не вполне ясно, кто отвечает за такую генерацию, учитывая, что модели генерируют контент на основе обучающих данных, но запрос генерирует пользователь. Является в целом стандартным потребовать у оператора ИИ-систем обеспечить наличие систем защиты от такого контента на уровне предобработки.
- Защита от использования в датасетах чужих информационных данных (и воспроизведения в результатах выдачи таких данных). За нарушение требований о локализации персональных данных, об их трансграничной передаче, о коммерческой тайне, а также обязательств, взятых перед третьими лицами, возможна существенная материальная ответственность.
- Наличие у ИИ-сервиса исключительных прав на (i) доработки (дообучение и надстройки для ИИ-моделей) — по принципу защиты прав на ПО; (ii) методы и способы дообучения моделей — по принципу защиты изобретений или ноу-хау; (iii) используемые данные — по принципу защиты прав на базы данных и лимитов для парсинга общедоступной информации в Интернете, включая нарушение чужих исключительных прав за счет использования контента, защищенного авторским правом.
- Текущие регуляторные риски — защита персональных данных, необходимость получения лицензий и разрешений в определенных законом случаях.
- По некоторым специальным контрактам на получение мощностей / API на модели с провайдерами может быть вендор-лок или реализоваться санкционные риски (например, при вступлении в таргет российского покупателя).
- Для моделей, оперирующих в специальных общественно значимых областях знаний (медицина, юри-

спруденция, финансы, строительство и т. д.), критически важно проверять наличие систем проверки «объяснимости» выдачи у ИИ-моделей (для возможности верификации и перепроверки качества работы), а также самоцензуры и цензуры нелегального контента. Важно понимать при этом, что 100% верификации результатов выдачи от модели быть не может.

- Отсутствие внутреннего локального нормативного акта, регулирующего как создание служебных произведений, так и использование ИИ при создании кода. ИИ уже как инструмент может использоваться сотрудниками халатно и, как следствие, влечь неработоспособность объектов, создаваемых с его помощью, и / или отсутствие прав на создаваемые объекты, равно как и репутационные риски. Урегулированность на уровне ЛНА уже может означать наличие систем контроля и осведомленность работников о красных линиях.
- Отсутствие системы мониторинга и устранения дрифта.
- Для некоторых ИИ-компаний имеются также специфические риски: риск тренировки собственных моделей с использованием API чужих моделей, уязвимость к хакерским атакам и утечкам, уязвимость в части компрометации модели и обратного извлечения из модели сведений, на которых она обучена / конфиденциальной информации, дрифт ML-моделей, иные технические параметры, соблюдение которых может быть дилбрейкером ввиду прямого влияния на работоспособность и различной возможности их устранения.



Владислав Лазуткин

старший юрист

ORION

> В сделках приобретения ИИ-активов стоит учитывать три фактора: (i) регулирование обработки персональных данных и данных, входящих в базы данных / содержащих проприетарную информацию (парсинг и т. п.), в коммерческих целях; (ii) условия использования иных AI-решений, в том числе мощных зарубежных языковых моделей (которые целевой бизнес может скрыто или явно использовать через API или иным образом); (iii) типичные проблемы с возможностью предоставления правовой защиты результатам генерации ИИ и оформлением таргетов прав на разработки.

2.1.1 Права на обучающие датасеты



#РЕЗУЛЬТАТЫ_ОПРОСОВ

По данным опроса, проведенного в ходе исследования, 90% респондентов наиболее важной областью проверки ИИ-компании считают слой данных ИИ-системы, в частности, вопросы, связанные с «чистотой» дообучающих датасетов базовой модели, использованной при разработке ИИ-системы.

По данным Опроса по аспектам Tech M&A.

Как показали приведенные результаты опроса, абсолютное большинство (**90%**) респондентов отметили слой обучающих данных, в частности, права на датасеты, в качестве приоритетной области проверки ИИ-компании.

Важно понимать, что относительно полноценную проверку, как юридическую, так и техническую, можно сделать **только в отношении данных, которые подконтрольны оператору системы**, т. е. к которым у него есть прямой доступ. В абсолютном большинстве случаев это не относится к данным, на которых предобучалась базовая модель.

Датасеты, на которых изначально обучалась модель (предобучающие данные), а также все последующие дообучающие выборки, которые использовал разработчик модели, проверить с точки зрения юридической «чистоты» невозможно. Это связано с закрытым характером большинства таких датасетов из-за высоких рисков раскрытия для их владельцев, а также усилением тренда на приватность предобучающих данных даже в тех случаях, когда ранее они могли быть открытыми[37].

[37] Например, при использовании некоторых моделей в полностью открытом формате.

#АНАЛИЗ_РИСКОВ #ОБУЧАЮЩИЕ_ДАННЫЕ

Поскольку ИИ-активы датацентричны, наиболее критичные и распространенные риски, как юридические, так и прочие, относятся к слою данных. В рамках ИИ-сервиса данные — это «топливо», формирующее знания и специализацию модели. Правовые дефекты, присущие датасетам, «наследуются» конечным продуктом. Поэтому в рамках юридического due diligence ИИ-системы вопросы обучающих данных занимают центральное место.

Ключевыми категориями таких рисков являются неблагоприятные последствия, связанные с:

Нарушением исключительных прав на чужие объекты интеллектуальной собственности

Использование при дообучении или ином формате адаптации модели ОИС без согласия правообладателей может привести к рискам взыскания крупных денежных штрафов или компенсаций, а также запрета использования спорных объектов.

Несоблюдением правил обработки персональных данных

Неправомерное включение в датасеты персональных данных без надлежащего основания их обработки создает риск привлечения к административной ответственности и крупным штрафам, в том числе оборотным.

Неавторизованным использованием информации ограниченного доступа

Неправомерный доступ и использование закрытой информации, включая коммерческую или иную охраняемую законом тайну, также может повлечь предъявление требований о взыскании убытков и иную ответственность.

Дефектами титула на датасеты[38], сформированные методами автоматизированного сбора (парсинга)

Автоматизированный сбор (парсинг) внешних информационных ресурсов, осуществленный в обход пользовательских соглашений, технологических барьеров или законодательных запретов, создает риск оспаривания легитимности происхождения всего массива данных, а также ставит вопрос о наличии титула на сформированный датасет.

Невозможностью эксплуатации ИИ-системы

Выявление факта несанкционированного использования охраняемых объектов или данных при дообучении или адаптации модели может привести к вынесению судом запрета на дальнейшее использование соответствующих данных.

[38] Этот риск был подробно рассмотрен в предыдущем разделе 1 главы 3 исследования «Периметр ключевых активов ИИ-компании в контексте M&A».

> **В отношении датасетов, на которых изначально обучалась базовая модель (т. н. массивов предобучающих данных), фактически нельзя провести полноценную техническую экспертизу и, тем более, — юридическую. Не имеет смысла запрашивать выборки из таких датасетов у оператора ИИ-системы, поскольку у него в абсолютном большинстве случаев нет к ним прямого доступа.**

На практике указанные риски обладают **свойством гиперкумулятивности**, они наслаиваются и усиливают друг друга. Датасет может одновременно содержать чужие ОИС, персональные данные и информацию с ограниченным доступом. В отличие от традиционных ИТ-продуктов, где объем проверяемых данных, включая охраняемый контент, имеет потенциально обозримые границы, ИИ-модели оперируют массивами данных, исчисляемыми миллиардами единиц. Это кратно увеличивает вероятность инкорпорирования «токсичного» элемента в обучающую выборку и, как следствие, масштаб потенциальной ответственности.

#ОБУЧАЮЩИЕ _ДАННЫЕ



Роман Головацкий

партнер

DÉNUO

Извлечение и локализация «токсичного» массива данных в уже дообученной модели технически, скорее всего, невозможны. В таких обстоятельствах единственным способом исполнения судебного запрета для владельца ИИ-системы может оказаться полное прекращение эксплуатации и удаление модели, «зараженной» неправомерными данными, или, как минимум, ее дообученной части. Это, в свою очередь, повлечет за собой причинение значительного ущерба или даже разрушение бизнеса, основанного на таком решении.

Ситуация становится еще более неразрешимой в случае, если модель используется в ИИ-сервисе удаленно, например через API. В таком случае владелец ИИ-сервиса вообще лишен возможности самостоятельно принять какие-либо меры в отношении модели (например, передообучить ее), поскольку она находится вне его инфраструктурного контура. В результате исполнение соответствующих требований может оказаться возможным лишь путем полного прекращения работы ИИ-сервиса.

При этом попытки ограничиться лишь изменением конфигурации инфраструктурного контура (например, переносом «зараженной» модели с одного сервера на другой) не только не обеспечат исполнение судебного запрета, но и могут повлечь новые нарушения, что, в свою очередь, способно стать основанием для предъявления дополнительных требований.

Таким образом, при приобретении ИИ-бизнеса покупатель должен учитывать последствия отсутствия юридической проверки «чистоты» слоя данных либо проведения такой проверки в неполном объеме. В то же время следует отметить, что в силу значительного объема данных, включенных в датасеты, их полная юридическая проверка может оказаться крайне времязатратной и дорогостоящей процедурой, а применение методов экстраполяции не позволяет полностью исключить соответствующие риски.



Шермет Курбанов

соруководитель практики интеллектуальной собственности и цифрового права

sll
SL LEGAL

Одним из основных правовых барьеров для коммерциализации ИИ-технологий остается вопрос законности обучения моделей на объектах авторского права (текстах, изображениях, коде). Мировая практика и регулирование в этой области находятся в стадии формирования.

Выделяют три основных правовых подхода к обучению ИИ:

- Обучение не считается использованием объекта авторского права, так как модель извлекает неохраняемые элементы и закономерности.
- Обучение является использованием, но может подпадать под установленные законом исключения и не требовать разрешения правообладателя.
- Обучение является использованием, требующим получения согласия от правообладателей.

В России специальных норм для ИИ пока нет. Существует позиция, что обучение само по себе не является нарушением, так как из произведений (объектов авторского права) извлекаются неохраняемые элементы. Тем не менее, есть и обратная аргументация, что охраняемые объекты могут условно «сохраняться» в параметрах обученной модели. Этот риск усиливается, если модель демонстрирует высокий «коэффициент запоминания» и начинает генерировать результаты, идентичные или существенно схожие с конкретными объектами из обучающей выборки. В условиях отсутствия сложившейся судебной практики такие случаи могут стать основанием для претензий правообладателей.

Отдельное внимание стоит уделить рискам, связанным с хранением исходного обучающего датасета. Вероятность признания такого хранения нарушением авторских прав достаточно высока, и этот фактор необходимо учитывать при структурировании сделки.

Аналогичная проблема возникает при использовании чужих баз данных. Несмотря на более слабый режим охраны, неправомерное извлечение (парсинг) содержимого таких баз (например, с крупных онлайн-плат-

форм) может быть признано нарушением. Кроме того, если материалы попали в базу данных изначально незаконно, пользователь такой модели автоматически наследует все риски неправомерного использования чужих объектов.

В связи с этим важно проверять, на каких данных дообучалась модель и как эти данные были получены. Как и в случае с персональными данными, если таргет не позаботился об этом, получить все необходимые правовые основания постфактум — достаточно сложная, если не невыполнимая задача. Поэтому критически важно выявить все нарушения и недостатки в работе таргета с интеллектуальной собственностью и учесть их при структурировании сделки.



Анатолий Земцов

управляющий партнер

dfcenter

Существует точка зрения, что прямой анализ нейросети не позволит установить, использовались ли при ее обучении конкретные объекты авторского права. Тем не менее серия экспериментов, проведенных в конце 2025 — начале 2026 гг. исследователями в сфере искусственного интеллекта это опровергает: с помощью специально подготовленных запросов они смогли «достать» из самых популярных коммерческих нейросетей до 90% оригинального текста нескольких известных произведений. Да, это пока еще «лабораторная» работа, потребовавшая большого количества итераций и перенастроек промптов. Но это показывает потенциальную возможность реализации такой задачи, а значит, вполне может скоро быть использовано и в прикладной экспертной практике. Что существенно повышает реализацию описанных выше рисков выявления в обучающих данных объектов прав третьих лиц.



Илья Булгаков
советник
DÉNUO

Если рассматривать упрощенно, то источников получения данных для развития ИИ-сервиса может быть три: собственные данные, данные сторонних сервисов (в том числе полученные через официальный API или публичные данные (в том числе полученные через парсинг открытых источников)). В зависимости от источника данных, разные аспекты потребуют более пристального внимания при проведении проверки.

- Если говорить про собственные данные, то в данном случае будут стоять вопросы соблюдения персональных данных (есть ли правовое основание для обработки для целей обучения ИИ), вопросы прав на такие данные (кому принадлежит исключительное право и охраняются ли такие данные в принципе).
- Если говорить про данные, полученные от третьих лиц, то основной акцент при проверке следует уделить на официальную документацию к API, соглашение об использовании API и получении данных, а также на накладываемые ограничения.
- Если речь идет об использовании публичных данных (о данных, полученных за счет парсинга), то этот вопрос один из самых сложных на практике, так как в данном случае получение «топлива» для обучения ИИ сопряжено как со сложными вопросами персональных данных, так и прав на базы данных.
    - Обучение ИИ требует больших объемов данных. Редко когда можно ограничиться лишь небольшим датасетом. Поэтому обычно при обучении компании парсят достаточно большие объемы данных, доступных в Интернете. Даже если использовать данные, которые как бы «ничьи» или которые сделаны публичными (например, публичные отзывы о товарах, данные из соцсетей), то все равно необходимо учитывать права так называемых владельцев баз данных.
    - Учитывая, что объем данных, извлекаемых, сохраняемых и используемых при обучении ИИ моделей, обычно достаточно большой и может состав-

лять терабайты данных, существует вероятность, что такие действия могут быть признаны нарушением смежных прав, если такая совокупность данных будет квалифицирована как база данных, а владельцы соответствующих сайтов — как их правообладатели.

ИИ-модели оперируют массивами данных, исчисляемыми миллиардами единиц. Это кратно увеличивает вероятность инкорпорирования «токсичного» элемента в обучающую выборку и, как следствие, масштаб потенциальной ответственности.

В ходе исследования мы также попросили **технических экспертов из DFCenter** рассказать о шагах, которые следует предпринять покупателю ИИ-бизнеса, чтобы проверить качество, объем, разметку (предподготовку), репрезентативность обучающих данных, и уточнить, действительно ли соответствующую информацию можно запросить только в отношении непосредственно тех данных, которые разработчик ИИ-системы использовал при адаптации сторонней ИИ-модели, но не в отношении предобучающего датасета.

#ТЕХНИЧЕСКАЯ_ЭКСПЕРТИЗА



Анатолий Земцов

управляющий партнер

dfcenter

Покупателю следует запросить описание источников данных, статистику распределений, метрики качества разметки, примеры выборок и результаты тестирования модели на независимых контрольных датасетах. На основании этих данных необходимо провести аудит баланса классов, полноты покрытия целевых сценариев и наличия шумов. Также желательна валидация модели не на предоставленных продавцом, а на собственных тестовых данных покупателя.

Важно четко понимать, что продавец сможет дать покупателю содержательные ответы и детальную информацию только в отношении тех данных, которые находились под его контролем и использовались им непосредственно: его собственные датасеты для дообучения, доразметки, фильтрации, калибровки или тестирования.

В отношении исходных обучающих датасетов базовой ИИ-модели продавец, как правило, не располагает полной информацией и не имеет возможности ее раскрывать, если он выступает интегратором или лицензиатом сторонней модели. Такие сведения контролируются разработчиком модели и часто охраняются коммерческой тайной. Либо он их в принципе не знает, т. к. лицензиар ему их не раскрывал.

Слой обучающих данных ИИ-системы

1. Ключевые области юридического due diligence

- Источники и способы получения обучающих выборок данных, использованных для дообучения и прочих форматов адаптации ИИ-модели.
- Состав и категории данных, использованных для дообучения или адаптации ИИ-модели иными методами.
- Текст соглашений, определяющих порядок и условия использования указанных данных, заключенных с владельцами таких данных.
- Текст документа, регламентирующего действия компании и ее работников в отношении сбора данных с использованием автоматизированных методов (в т. ч. парсинга), обработки и использования таких данных.

2. Ключевые red-flag риски

- Датасеты, использованные при дообучении ИИ-модели, содержат объекты авторских прав в отсутствие разрешений их авторов или иных правообладателей. Может привести к требованиям о взыскании компенсаций, запрету использования ИИ-модели и прикладных решений, созданных на ее основе, включая мультиагентные системы.
- В состав обучающих выборок были включены персональные данные, собранные и обрабатываемые без согласия субъектов персональных данных или иного правового основания. Может привести к взысканию штрафов, блокировке дальнейшей обработки персональных данных.
- ИИ-модель была дообучена на данных, полученных посредством парсинга социальных сетей с нарушением условий использования соответствующих платформ. Может привести к оспариванию титула на соответствующий датасет, запрету использования ИИ-модели, взысканию компенсаций.

2.1.2 Условия использования ИИ-моделей



Считают приоритетной юридическую проверку условий использования внешних ИИ-моделей

#РЕЗУЛЬТАТЫ_ОПРОСОВ

По итогам опроса, проведенного в ходе исследования, 76% респондентов приоритетной областью проверки ИИ-компании считают условия использования базовых моделей сторонних разработчиков, интегрированных в ИИ-систему.

По данным Опроса по аспектам Tech M&A.

Слой базовой модели, использованной в ИИ-системе, также очень важен с точки зрения анализа юридических рисков. Но возможность управления такими рисками существенно ограничена условиями использования модели.

Базовую модель создавало третье лицо — ее разработчик, который не является участником сделки, для целей которой проводится due diligence прикладного ИИ-решения. Он — лишь поставщик важного (а в случаях, когда нужно использовать модель конкретного семейства — критически важного) ресурса. В рамках юридической проверки можно проверить только условия и ограничения использования этого ресурса.

Абсолютное большинство базовых моделей распространяется по стандартизированным лицензиям, присоединяющаяся сторона не может влиять на их содержание. Разработчик системы может лишь выбирать контрагента (провайдера модели), оценивать свои риски, исходя из условий использования модели и дополнительно раскрытой информации, и принимать решение об использовании модели или отказе от нее.

Покупатель ИИ-компании имеет схожий набор опций управления такими рисками. При выявлении неприемлемых рисков покупатель ИИ-компании может либо отказаться от сделки, либо попросить продавца заменить модель или сделать это самостоятельно, принимая при этом большинство исторических рисков, связанных с прежней моделью.

#АНАЛИЗ_РИСКОВ #БАЗОВАЯ_МОДЕЛЬ

Основные риски использования сторонней базовой модели могут вытекать из следующего[39]:

- **Договор об использовании базовой модели заключен неуполномоченным лицом.**

  Необходимо убедиться, что именно приобретаемая компания является стороной соответствующего договора. Если лицензия платная — следует проверить, что платежи выплачиваются компанией и отсутствуют препятствия (например, санкционные ограничения) для совершения платежей после ее перехода в группу покупателя.

- **Модель используется с нарушением лицензионных ограничений.**

  Если условия соглашения не позволяют использовать модель в целях или способами, которыми ее использует приобретаемая компания (в контексте ее бизнеса) или которыми планирует покупатель, — такое использование будет неправомерным и может повлечь штрафные санкции, взыскание компенсаций, прекращение лицензии и доступа к модели.

- **Разработчик модели имеет право использовать пользовательские данные для развития модели.**

  В этом случае разработчик системы, использующий для адаптации модели собственные наборы данных, рискует утратить конкурентное преимущество, создаваемое с помощью таких данных. Также это может привести к утечке конфиденциальных и чувствительных данных, в том числе клиентских, и утрате контроля над тем, как они будут использованы в будущих версиях модели.

- **Пользователь не вправе дообучать модель или может это делать в строго ограниченных форматах.**

  Такие условия могут снизить коммерческую привлекательность текущего и будущего продуктов. Также невозможность дообучения модели может привести к ее скорой деградации, например, по причине дрейфа.

- **Соглашение не регулирует вопрос принадлежности прав на результат дообучения модели или указывает на его принадлежность разработчику модели.**

  В этом случае владелец ИИ-системы не может контролировать качество, работоспособность и конфиденциальность результата дообучения модели, а также распоряжаться таким результатом как самостоятельным активом.

- **Модель является производной, но предыдущий дообучатель нарушил условия соответствующей лицензии или проверка таких условий затруднена.**

[39] Более подробно возможные риски использования базовой модели при создании и эксплуатации ИИ-системы рассмотрены в разделе 1 главы 3 исследования «Периметр ключевых активов ИИ-компании в контексте M&A».

Если в основе ИИ-системы лежит производная ИИ-модель, это создает риск предъявления претензий со стороны правообладателя исходной базовой модели, включая требования о прекращении ее использования, об изъятии с рынка конечного продукта, выплате компенсаций и штрафных санкций.

- **Условия распространения модели требуют раскрытия исходного кода всего решения, в которое модель была интегрирована.**

  При интеграции такой модели в собственный проприетарный продукт компания может быть вынуждена обнародовать весь исходный код своего решения, что лишает его конкурентных преимуществ, поскольку сокращает возможности коммерческого лицензирования конечного продукта.

- **Модель является зарубежной (разработана иностранным вендором или находится под его контролем).**

  Это создает риски невозможности использования решений на ее основе на объектах КИИ и при исполнении контрактов с предприятиями государственного сектора из-за требований импортозамещения, санкционных и регуляторных ограничений, что может привести к отказу в допуске к участию в тендерах, блокировке проекта или расторжению контракта заказчиком.

- **Модель несовместима с некоторыми другими решениями.**

  Если покупатель планирует добавить в приобретаемый продукт дополнительные сторонние ИИ-модели или его ИТ-контур не позволяет интегрировать такое решение без изменения технологического стека, вопросы совместимости могут быть критичны.

- **Ответственность разработчика модели за любые инциденты полностью исключена.**

  Это означает, что при возникновении убытков из-за ошибок модели (например, при выдаче дискриминационных или необоснованных решений, утечке чувствительных данных) приобретаемая компания не сможет взыскать компенсацию с разработчика модели в порядке регресса и будет вынуждена самостоятельно нести все имущественные потери, вызванные таким инцидентом.

> **Базовую модель создавало третье лицо — ее разработчик, который не является участником сделки M&A с другим субъектным составом. Он — лишь поставщик важного ресурса. В рамках юридической проверки можно проверить только условия и ограничения использования этого ресурса, все остальные вопросы, связанные с его «производством», — зона влияния стороннего лица, которое не связано обязательствами по раскрытию этой информации в рамках сделки других игроков.**

#БАЗОВАЯ_МОДЕЛЬ



Алексей Дарков

советник, руководитель практики «Интеллектуальная собственность»

VERBA LEGAL

Данный вопрос действительно заслуживает внимания при проверке ИТ-компаний: при использовании моделей внешних провайдеров (OpenAI, Google, Claude и др.) компания часто передает собственные данные в облако.

Если лицензионное соглашение позволяет провайдеру использовать эти данные для улучшения своей модели, компания рискует не только раскрыть конфиденциальные алгоритмы, но и передать конкурентам коммерческие секреты. Классический пример — скандал с Samsung, когда сотрудники загружали конфиденциальный код в ChatGPT.

Кроме того, контент, генерируемый ИИ, может нарушать исключительные права третьих лиц — например, GitHub Copilot часто обвиняют в нарушении условий open source лицензий, а Midjourney — в нарушении прав на изображения. При этом дальнейшее использование таких объектов непосредственной компанией также является нарушением исключительных прав. Для минимизации аналогичных рисков разумно учитывать, содержат ли условия использования заверения об обстоятельствах или возможность возмещения убытков.



Илья Булгаков

советник

DÉNUO

При проведении юридического due diligence компании, которая строит свой бизнес вокруг использования ИИ, необходимо детально анализировать, какую конкретно модель или модели использует компания.

- Если речь идет о том, что компания использует open source модель (а это достаточно распространенная ситуация, особенно после того, как все больше и больше провайдеров распространяют свои модели на условиях open source), то необходимо детально проанализировать как сами лицензионные условия такой модели, так и условия моделей, на ос-

нове которых она была в свою очередь создана. Необходимо проследить всю историю создания модели (историю «наследования» моделей), которая используется таргетом, и проверить всю цепочку лицензий, чтобы установить, что компания может коммерциализировать свою деятельность.

- Лицензионные условия open source моделей также обладают своей спецификой, что в целом не такая редкая ситуация. Очень часто включаются условия о запрете для использования для улучшения конкурирующих моделей, ограничения на размер выручки и пользователей после которых лицензия становится платной, ограничения по юрисдикции из-за санкционных ограничений, ограничения на этическое использование. Соответственно, при анализе лицензий генеративных моделей необходимо внимательно изучить бизнес таргета и проанализировать как текущие ограничения, так и ограничения, которые могут быть в будущем, если продукт будет развиваться и расти.
- Следует также учитывать, что если российская компания выбирает строить свой продукт на основе open source модели, то зачастую такие модели разрабатываются иностранными научными институтами и имеют ограничения research only или academic use only. Иными словами, коммерческое использование в принципе запрещено.

Другим вопросом является соблюдение лицензионных ограничений при использовании моделей, доступ к которым предоставляют сторонние провайдеры. Помимо анализа условий того, кому принадлежат права на результат, созданный такой моделью, зачастую условия использования содержат ограничения на использование (например, ограничения на количество запросов к модели). При нарушении таких условий обычно провайдерами блокируется доступ к модели, что приводит к остановке бизнеса.



Софья Смирнова

советник M&A
и корпоративной практики

O_2 консалтинг

Если компания использует сторонние ИИ-модели или API, важно проверять, какие права ей предоставлены, можно ли использовать внешний продукт в коммерческих целях, возможна ли интеграция модели в собственный продукт, существуют ли ограничения по территории, количеству пользователей или видам деятельности. На практике существенное значение имеют также ограничения на использование модели в отдельных отраслях и право провайдера изменять функциональность модели или тарифные условия. Для многих ИИ-компаний критическим риском является ситуация, при которой изменение стоимости API, лимитов запросов или правил доступа к модели способно напрямую повлиять на экономику продукта или привести к необходимости срочной перестройки всей технической инфраструктуры.

> **Базовые модели распространяются на основании условий, к которым пользователь зачастую лишь присоединяется, но не может влиять на их содержание. Поэтому на этапе due diligence важно попытаться понять все доступные опции бесшовной с технической и юридической точек зрения замены модели на другую, если текущие условия использования модели не будут соответствовать коммерческим целям приобретателя ИИ-бизнеса.**

Мы попросили **Анатолия Земцова** (DFCenter) рассказать о ключевых технических параметрах ИИ-модели, информацию о которых покупателю ИИ-бизнеса следует запросить у продавца для целей юридического и технического due diligence.

#ТЕХНИЧЕСКАЯ_ЭКСПЕРТИЗА



Анатолий Земцов

управляющий партнер

dfcenter

Ключевые параметры: архитектура модели, число параметров и слоев, размер весов, используемые алгоритмы обучения, метрики точности, устойчивость к шуму, требования к инфраструктуре. Для коммерческой эксплуатации необходимы пайплайны дообучения, система мониторинга качества и дрифта, журналирование запросов и механизм обновления модели. Без этого модель быстро потеряет прикладную ценность.

Однако стоит оговориться, что все эти параметры может представить только разработчик самой модели. А вот владелец ИИ-сервиса (продавец), построенного «поверх» такой модели — далеко не всегда. Продавцу могут быть доступны только некоторые из перечисленных данных (параметров). Какие конкретно — зависит от технической и юридической модели взаимодействия продавца и провайдера (владельца модели).

Слой базовой модели

1. Ключевые области юридического due diligence

- ИИ-модель (модели), используемая(-ые) в основе системы, с указанием идентифицирующих сведений, включая наименование, разработчика / правообладателя, версию, и способ распространения.
- Текст соглашения, на основании которого осуществляется использование ИИ-модели, либо ссылка на применимые условия публичной лицензионной оферты, правила использования или открытую лицензию.
- Способы интеграции и использования ИИ-модели, включая сведения о том, развернута ли модель в локальном контуре или предоставляется удаленно через инфраструктуру (сервис) провайдера.
- В случае использования производной модели, дообученной третьим(-ими) лицом(-ами), — тексты всех соглашений (или ссылки на них), опосредующих «цепочку» использования и дообучения модели, начиная с исходного правообладателя.
- Внутренние регламенты (политики), определяющие порядок использования и фиксации прав на результаты генерации ИИ-системы.

2. Ключевые red-flag риски

- Имеющаяся у таргета лицензия не позволяет использовать ИИ-модель в коммерческих целях. Может привести к отзыву лицензии, требованиям о взыскании компенсаций, запрету использования ИИ-модели.
- Правообладателем ИИ-модели установлен запрет на ее использование для деятельности, осуществляемой таргетом. Может привести к отзыву лицензии, требованиям о взыскании компенсаций, запрету использования ИИ-модели.
- Лицензионные условия предъявляют требования о раскрытии исходного кода решения, в которое интегрируется ИИ-модель. Неисполнение требований может привести к отзыву лицензии, запрету использования ИИ-модели.
- Компания не может дообучать модель или адаптировать ее иным образом без существенного риска утраты контроля над принадлежащими ей данными, включая чувствительную информацию.
- Компании не принадлежит результат дообучения модели и право распоряжения им, в том числе в случае, если у нее есть экземпляр дообученных весов или правомерный доступ к ним.

2.1.3 Защита персональных данных



Считают ключевой областью проверки ИИ-компании вопросы защиты персональных данных

#РЕЗУЛЬТАТЫ_ОПРОСОВ

По данным опроса, проведенного в ходе исследования, 37% респондентов наиболее важной областью проверки ИИ-компании считают вопросы, связанные с защитой персональных данных.

По данным Опроса по аспектам Tech M&A.

Своего рода константой и обязательным элементом как обучения, так и дообучения ИИ-моделей является предварительный сбор, подготовка и анализ широкого массива данных. Эти данные могут включать персональные данные. Развитие ИИ-технологий стало одной из причин роста инцидентов, связанных с утечками персональных данных. В 2025 г. эта тенденция лишь усилилась по мере появления все большего числа доступных ИИ-решений.

Для большинства ИИ-продуктов наличие персональных данных в обучающей (дообучающей) выборке излишне: не улучшает эффективность и не снижает негативные эффекты. В таких случаях персональные данные могут удаляться из датасетов на стадии подготовки данных. Тем не менее, на практике персональные данные могут остаться нетронутыми. Кроме того, учитывая объемы данных, исключить все персональные данные — крайне сложная задача. Наконец, для некоторых ИИ-продуктов наличие данных и их привязка (хотя бы частичная) играет важную роль с точки зрения качества и эффективности модели.

Наличие неустраненного риска (обработка персональных данных без надлежащего основания) на стадии сбора данных (формирования «сырого» датасета) — может приводить к его сохранению или увеличению на других стадиях жизненного цикла ИИ-системы: (i) подготовки данных (формирование «вторичных / очищенных» датасетов); (ii) «хранения» персональных данных в параметрах обученной (дообученной) ИИ-модели.

Также вопросы персональных данных могут возникать при добавлении в ИИ-систему дополнительных элементов поверх чужой ИИ-модели (например, RAG) и при непосредственной эксплуатации (пользовательские промпты). Оператор ИИ-системы зачастую не способен контролировать эти вопросы на стадии сбора, подготовки и использования предобучающего датасета для создания базовой модели, но способен контролировать их в своем контуре (при дообучении, добавлении дополнительных элементов поверх ИИ-модели и последующей эксплуатации ИИ-системы).

#АНАЛИЗ_РИСКОВ #ПЕРСОНАЛЬНЫЕ_ДАННЫЕ

Большинство рисков в сфере персональных данных при использовании ИИ-технологий связаны с:

- **Отсутствием надлежащего основания обработки ПДн**

  в процессе создания и эксплуатации ИИ-системы, включая стадию сбора данных, на которой проводилось формирование обучающего датасета. Это самый распространенный риск, который может приводить к штрафным санкциям и требованиям о прекращении обработки ПДн.

- **Нарушением принципов обработки ПДн**

  Частным примером такого нарушения является ситуация, когда в согласии на обработку ПДн явным образом не указываются цели их обработки, связанные с эксплуатацией ИИ-системы — подготовка данных, включая разметку и очистку, обучение и дообучение модели.

- **Нарушением требований к трансграничной передаче ПДн**

  в процессе функционирования ИИ-системы, если она основана на зарубежных моделях, которые не были локализованы. Может повлечь штрафные санкции, запрет на трансграничную передачу, а также ограничение доступа (блокировку) к сервису оператора на территории РФ.

- **Нарушением требований к локализации ПДн российских граждан**

  Наказывается штрафом до 6 млн руб. (за повторное нарушение — до 18 млн руб.) и может повлечь принудительную блокировку информационного ресурса оператора на территории РФ по требованию Роскомнадзора.

- **Отсутствием в компании комплекса технических и организационных мер,**

  направленных на предотвращение утечек ПДн в связи с использованием ИИ-технологий, а также системы адекватного реагирования на соответствующие инциденты. Непринятие необходимых мер, включая применение средств DLP, обезличивание данных, контроль доступа и внутренний мониторинг, при наступлении утечки ПДн квалифицируется как нарушение требований к защите ПДн и влечет штрафы, размер которых зависит от масштаба утечки.

#ПЕРСОНАЛЬНЫЕ_ДАННЫЕ



Роман Головацкий

партнер

DÉNUO

В ходе проверки решений на основе ИИ, помимо анализа принадлежности правового титула на соответствующее ПО и результаты его использования, а также прав на датасеты и иные входные данные, особое внимание уделяется изучению того, каким образом выстроена архитектура решения и порядок обработки данных. Так, например, если разработчик в составе своего продукта использует внешний ИИ сервис вместо или в дополнение к локально развернутым ИИ моделям, то в этом случае проверка должна охватывать оценку следующих проблем:

1. Обеспечение конфиденциальности коммерчески чувствительной информации и предотвращение ее несанкционированного раскрытия третьим лицам, включая провайдера сервиса;
2. Соблюдение требований по обработке персональных данных, включая трансграничные передачи и требования к локализации баз данных;
3. Соответствие применения внешнего ИИ-сервиса в составе анализируемого решения условиям использования такого сервиса, лицензиям и ограничениям, включая ограничения на обработку входных данных и ограничения на использование результатов работы сервиса.



Шермет Курбанов

соруководитель практики интеллектуальной собственности и цифрового права

sll
SL LEGAL

Особое внимание привлекают вопросы персональных данных, возникающие в связи с использованием обучающих датасетов и данных, «встроенных» в модель (хотя обученная модель не хранит исходные данные напрямую, она усваивает информацию из них и может опосредованно воспроизводить характеристики и элементы исходных данных). Эти вопросы требуют пристального внимания и проработки.

- При покупке ИИ-таргета риски, связанные с персональными данными, могут возникать как в отношении обучающего датасета, так и в отношении самой модели, потенциально «сохраняющей» такие данные.
- Важно заранее выявить соответствующие риски и проверить соблюдение требований законодательства о персональных данных. Необходимо проверить ряд моментов, в частности: (i) локализацию (хранение собранных персональных данных российских граждан в России); (ii) трансграничную передачу (передачу данных лицам за рубежом); (iii) автоматизированное принятие решений (запрет принимать решения, имеющие юридические последствия для человека, исключительно автоматически и без его согласия).
- Указанные риски могут с разной степенью важности возникать в зависимости от конфигурации сделки и вида продаваемого таргета. Однако наиболее критичным остается наличие правовых оснований для обработки персональных данных, включенных в обучающий датасет. Таргет вправе обрабатывать данные физических лиц только при наличии таких оснований (например, согласия или законного интереса). Этот вопрос является самым чувствительным для таргета и наиболее важным для покупателя. Многие другие нарушения можно исправить, тогда как отсутствие правового основания для обработки персональных данных — как правило, нет.
- Нарушение требований законодательства о персональных данных может привести к административным штрафам, а в отдельных случаях — к блокировке

ресурса (существует и уголовная ответственность, но в отсутствие преступного умысла о высокой общественной опасности такой сценарий маловероятен) и даже полному удалению ИИ-модели (что хоть и маловероятно, но не исключено).

Учитывая объемы данных, исключить персональные данные из любого обучающего датасета – крайне сложная задача. Оператор сторонней ИИ-системы не способен влиять эти вопросы на стадии сбора, подготовки и использования предобучающего датасета базовой модели, но может контролировать их в своем контуре (при дообучении, добавлении дополнительных элементов поверх ИИ-модели и последующей эксплуатации ИИ-системы).



Илья Булгаков

советник

DÉNUO

Первым вопросом стоит аспект соблюдения законодательства о локализации. Необходимо оценить не только то, насколько сам вендор модели должен и будет исполнять требования о локализации персональных данных, но и то, насколько данное требование будет соблюдаться при реализации технологического решения самой компанией. Требование о локализации устанавливает, что первичная база данных должна быть создана в России в момент сбора персональных данных граждан Российской Федерации. Это означает, что, например, иностранные вендоры, осуществляющие свою деятельность в России, обязаны выполнять требования о локализации, иначе они могут быть заблокированы на территории России.

Вторым вопросом стоит трансграничная передача данных. Многие провайдеры моделей зарегистрированы за границей. Если компания передает такой модели персональные данные для обработки, в этом случае происходит трансграничная передача персональных данных.

С 1 марта 2023 г. необходимо уведомлять Роскомнадзор о трансграничной передаче персональных данных. Уже было несколько решений о запрете трансграничной передачи. Следовательно, при использовании зарубежных компаний, предоставляющих услуги по доступу к своим моделям, размещенных на иностранных серверах, необходимо проанализировать, какие данные могут передаваться такой компании и необходимо ли уведомить Роскомнадзор.

Можно выделить несколько основных стадий «жизненного цикла» модели: (i) сбор данных для обучения модели; (ii) предпроцессинг данных и подготовка их к «скармливанию» модели; (iii) обучение модели; (iv) написание запросов (промптов) и получение ответов от модели, а также пост-обучение модели через обращения к ней через интерфейс (промпты).

Первые три стадии представляют наибольшую опасность с точки зрения прав и законных субъектов персональных данных. Зачастую для обучения компании берут данные в открытом доступе, а также собственные накопленные данные. В России для сбора открытых данных компаниям приходится полагаться на законный интерес как правовое основание для обработки в условиях отсутствия правоприменительной практики. Если используемый для дообучения модели USG-контент содержит персональные данные, то у компании возникает необходимость обоснования собственного правового обоснования для их сбора и обработки.

Российские компании также формально могут быть обязаны соблюдать требования GDPR, если они при работе с языковыми моделями используют персональные данные, которые охраняются в соответствии с нормами GDPR. Например, речь может идти о случаях, когда российская компания при подготовке датасета для дообучения или для других целей при работе с языковой моделью использует данные, полученные с помощью скраппинга ресурсов, которые очевидно содержат данные резидентов ЕС или используют персональные данные, полученные от иностранных контрагентов из ЕС.

Когда компания использует свои собственные данные, накопленные массивы данных самой компании, скорее всего, будут содержать персональные данные. Следовательно, в зависимости от того, данные каких субъектов собираются, необходимо обеспечить наличие правового основания. В большинстве случаев это будет согласие, в котором должны быть указаны такие цели обработки, как обучение модели, возможный предпроцессинг и разметка данных, а также дообучение модели в процессе использования.

Самым крупным риском для разработчиков ИИ-решений является возможность приостановки и блокировки Роскомнадзором обработки персональных данных, собранных с нарушением закона. Такое право прямо указано в законе и фактически может означать запрет на использование сервиса. Хотя о такой практике нам не известно, но формально такой риск существует.

#МНЕНИЕ_ЭКСПЕРТОВ

Анатолий Земцов (DFCenter) рассказал, можно ли с помощью методов технической экспертизы определить, содержит ли конкретный датасет персональные данные или, например, чужие ОИС, а также о необходимых условиях для проведения такой экспертизы.

#ТЕХНИЧЕСКАЯ_ЭКСПЕРТИЗА



Анатолий Земцов

управляющий партнер

dfcenter

Сегодня техническая экспертиза позволяет выявить персональные данные с помощью автоматических классификаторов и регулярных шаблонов, а также обнаружить защищенные ОИС через fingerprint-анализ и сравнение с известными общедоступными образцами. Это стандартная процедура data compliance-аудита. Однако окончательная юридическая квалификация требует дополнительно правового анализа, то есть привлечения ИТ-юриста.

Полноценная техническая экспертиза на предмет наличия персональных данных или объектов интеллектуальной собственности возможна только в отношении того датасета, к которому обеспечен фактический доступ (желательно — к полной версии, а не к выборке). Автоматические методы выявления персональных данных, сопоставление с известными источниками, fingerprint-анализ и иные процедуры требуют прямого анализа массива данных.

Если доступ отсутствует, возможен лишь косвенный аудит — анализ документации, описаний источников, процедур комплаенса и гарантий поставщика. Однако такой анализ не позволяет достоверно установить фактическое содержание датасета и не заменяет техническое исследование самого массива данных.

Персональные данные

1. Ключевые области юридического due diligence

- Использование компанией в рамках эксплуатации ИИ-системы зарубежных сторонних ИИ-моделей посредством удаленного доступа (формат cloud).
- Связь сферы функционирования ИИ-системы с обработкой специальных (чувствительных) категорий ПДн (например, медицинских), согласие на обработку которых требует письменной формы. Проведение дообучения ИИ-модели на таких данных под контролем компании.
- Адреса физического расположения баз данных, используемых для сбора и дальнейшей обработки ПДн пользователей ИИ-системы.
- Информация о передаче ПДн, обрабатываемых ИИ-системой, за пределы РФ с указанием юрисдикций-получателей, а также сведения об уведомлении Роскомнадзора о трансграничной передаче таких ПДн.
- Тексты согласий субъектов ПДн на использование их данных для целей дообучения ИИ-модели или подтверждение наличия иных правовых оснований для обработки ПДн в указанных целях.
- Подтверждение внедрения компанией мер и процедур, направленных на предотвращение утечек ПДн, в том числе при создании, эксплуатировании и использовании ИИ-системы, и их описание.
- Текст ЛНА или иного документа, принятого в компании, регламентирующего порядок обращения работниками с ПДн при использовании ИИ-системы. Наличие в нем запрета на загрузку необезличенных ПДн в ИИ-систему, а также их передачу в контур модели, если она не локализована.
- Применяемая в компании система реагирования на утечки, компрометацию и прочие инциденты, связанные с ПДн, обрабатываемыми при использовании ИИ-системы.
- Использование компанией каких-либо инструментов, направленных на техническую блокировку передачи ПДн во внешний контур (например, DLP-системы), их обезличивание / маскировку перед загрузкой в обучающую среду, или иных технологий защищенной обработки данных в процессе эксплуатации ИИ-системы.

2. Ключевые red-flag риски

- Нарушение требований о локализации баз данных, используемых для обработки ПДн при эксплуатации ИИ-системы. Может привести к значительным штрафным санкциям (от 6 до 18 млн руб.), блокировке информационного ресурса.
- Трансграничная передача ПДн в процессе работы ИИ-системы в юрисдикцию без уведомления / разрешения Роскомнадзора. Может привести к штрафным санкциям (исходя из последней практики размер штрафа может быть до 300 тыс. руб.), запрету дальнейшей передачи, блокировке ресурса.
- Обработка ПДн осуществляется без надлежащего правового основания. Может привести к штрафным санкциям (до 300 тыс. руб. и до 700 тыс. руб., если осуществлялась обработка специальных категорий или биометрических ПДн), приостановлению / блокировке обработки ПДн.

2.1.4 Условия использования инфраструктуры



Считают приоритетной юридическую проверку условий использования инфраструктуры и вычислительных мощностей

#РЕЗУЛЬТАТЫ_ОПРОСОВ

По данным опроса, проведенного в ходе исследования, 32% респондентов в качестве ключевых областей юридической проверки ИИ-компании отметили вопросы, связанные с условиями использования инфраструктуры (хранилищ данных и репозиториев системы), а также вычислительных мощностей.

По данным Опроса по аспектам Tech M&A.

В процессе юридического due diligence слоя инфраструктуры ИИ-системы важно подтвердить наличие у компании физического контроля (и определить его степень) над средой развертывания ИИ-системы и дообучения модели. Это требует тщательного анализа договоров с провайдерами вычислительных мощностей и инфраструктуры развертывания и хранения системы.

Только наличие доступа к вычислительному контуру, системам хранения данных и сетевая сегментация позволяет оператору ИИ-системы реализовать строгие требования SLA и обеспечить контроль над утечками данных. Чем выше целевой уровень доступности и изолированности ИИ-системы, тем важнее исключить внешние зависимости, существенно затрудняющие мониторинг и аудит безопасности. Если инфраструктура не обеспечивает полный эксплуатационный цикл ИИ-системы в закрытом контуре, риски утечек конфиденциальной информации и снижения качества модели становятся практически неуправляемыми.

Наибольший риск для ИИ-компании представляет использование сторонней модели в облачном формате, например, посредством API. Такая зависимость от провайдера модели уже сама по себе является уязвимостью. Облачная архитектура модели не позволяет оператору системы независимо дообучать и адаптировать ее на собственных данных, контролировать ее поведение и гарантировать заявленный уровень поддержки (SLA). Все ключевые функции сосредоточены во внешней инфраструктуре с непрозрачными параметрами безопасности. Риски могут включать утечку данных через API, одностороннее изменение условий или внезапное отключение сервиса, что для целей сделки M&A может иметь критическое значение.

Для оператора ИИ-системы, планирующего самостоятельное дообучение базовой модели на собственных данных, также **критически важно обеспечить наличие соответствующих вычислительных ресурсов** — графических ускорителей (GPU) с достаточным объемом видео-

памяти, высокопроизводительных СХД с низкой задержкой, а также масштабируемой сетевой инфраструктуры. Если по итогам due diligence будет выявлено отсутствие у компании таких мощностей, или расходы на эти цели не будут учтены в программе капитальных затрат, то при отсутствии таких возможностей в ИТ-контуре покупателя эти факторы могут повлечь неблагоприятные последствия.

Если дообучение модели требуется в рамках одного из этапов программы развития продукта, например, для целей его дальнейшей специализации, — его будет невозможно осуществить в разумные сроки без необходимости многократного увеличения расходов.

Если по тем или иным причинам (например, в результате необходимости экономии соответствующих незапланированных расходов) объем мощностей окажется недостаточным, оператор либо будет вынужден отказаться от дообучения, теряя конкурентное преимущество, либо столкнется с регулярными сбоями, потерями данных и невозможностью использования результатов дообучения. В контексте сделки M&A эти обстоятельства могут существенно снизить стоимость бизнеса, поэтому они требуют тщательного предварительного анализа.

#АНАЛИЗ_РИСКОВ #ВОПРОСЫ_ИНФРАСТРУКТУРЫ

К основным юридическим и регуляторным рискам, связанным с условиями использования инфраструктуры ИИ-системы, относятся следующие:

- **Временная миграция данных за пределы РФ на другие сервера, физически расположенные за рубежом**

  (например, в случае инцидентов), даже если используется отечественный дата-центр. Такая миграция будет считаться трансграничной передачей данных, даже если они физически не покидают основной ИТ-контур, но реплицируются на внешних серверах провайдера хостинга. Неуведомление Роскомнадзора о такой передаче может привести к штрафным санкциям и блокировке ИИ-системы.

- **ИИ-система развернута в российском ЦОДе, но средства мониторинга резервного копирования или технологической поддержки управляются с зарубежных IP-адресов**

  В данном случае также будет осуществляться трансграничная передача данных, что, соответственно, потребует соблюдение условий ее совершения (уведомление Роскомнадзора). В противном случае могут последовать штрафные санкции и блокировка системы.

- **Инфраструктурный контур использует зарубежные облачные решения, физическое расположение серверов внутри РФ не закреплено договором**

  и может быть изменено провайдером в одностороннем порядке. Это создает риск автоматической репликации данных на сервера за рубежом при балансировке нагрузки или резервном копирова-

нии, и, соответственно, риск нарушения требований трансграничной передачи данных или их локализации.

- **Отсутствие у провайдера внешней инфраструктуры сертификатов соответствия требованиям отечественных регуляторов**,

  если ИИ-система обрабатывает биометрические или специальные категории ПДн. Это влечет риск административных штрафов и предписание о приостановке обработки ПДн до устранения нарушений.

- **Хранение логов доступа и журналов событий системы только у провайдера инфраструктуры**

  без их репликации оператору ИИ-системы (компании). При утечке оператору системы будет сложно доказать, что нарушение произошло по вине провайдера, и взыскать с него компенсацию в размере уплаченного штрафа в порядке регресса.

- **В договоре с провайдером не урегулирован порядок экстренного доступа к инфраструктуре и передачи носителей информации по требованию государственных органов**

  При получении запроса на предоставление носителей с ПДн провайдер может воспрепятствовать их изъятию, и оператор будет привлечен к ответственности за невыполнение законного требования, а эксплуатация системы может быть приостановлена до исполнения требования.

- **В договоре с провайдером инфраструктуры отсутствует условие о праве оператора на проведение независимого аудита безопасности и физического доступа к серверам хранения**

  В таком случае оператор не сможет проверить реальные меры защиты ПДн, декларируемые провайдером, что может быть квалифицировано Роскомнадзором как непринятие надлежащих организационных мер по защите ПДн с наложением штрафа.

#ВОПРОСЫ_ИНФРАСТРУКТУРЫ



Илья Булгаков

советник

DÉNUO

Один из самых важных аспектов на ближайшие годы. Это связано с тем, что для работы генеративных моделей нужны, как правило, GPU (а не CPU), то есть достаточно мощные графические процессоры. Помимо того, что в принципе работа языковых моделей может потребовать значительных вычислительных мощностей, может сказаться также дефицит GPU у провайдеров. В этой связи имеют значение долгосрочные договоры с провайдерами GPU (дата-центры) либо наличие собственных GPU-серверных мощностей, способных обеспечить работу модели, ее обучение и дообучение.

Отдельным вопросом стоит финансовая составляющая договоров с дата-центрами. Вполне вероятен рост цен на их услуги вследствие возрастающего спроса, поэтому наличие долгосрочных договоренностей о цене за услуги дата-центров также является важным аспектом при проверке.



Алексей Дарков

советник, руководитель практики «Интеллектуальная собственность»

VERBA LEGAL

Если ИИ-компания построена на инфраструктуре стороннего провайдера с недостаточными гарантиями, срыв сервиса может стоить в разы дороже, чем сама компания. Попытка миграции на другую платформу потребует переписывания архитектуры и может занять месяцы. В контексте санкций и ухода с рынка многих поставщиков проблема стоит еще острее: никто не может гарантировать, что зарубежный поставщик не прекратит предоставление инфраструктуры, не компенсировав при этом убытки. Такие ситуации уже были предметом рассмотрения судов, не так давно Верховный Суд РФ давал разъяснения про ответственность дистрибьюторов в случае прекращения технической поддержки зарубежной компанией-правообладателем (дело № А56-24038/2024).

В сфере юридической проверки низкий приоритет может быть объясним бизнес-риском. Риск прекращения доступа к инфраструктуре вряд ли может быть закрыт правовыми конструкциями. Поэтому на первый план выходит оценка бизнес- и технических подходов зависимости от сторонней инфраструктуры. Тем не менее, лучше заранее уделять внимание вопросам исполнения и расторжения договоров на использование инфраструктуры и вычислительных мощностей, минимизировав риски.



Софья Смирнова

советник M&A
и корпоративной практики

O_2 консалтинг

Для ИИ-компаний критически важны условия предоставления облачной инфраструктуры и / или GPU-мощностей, поскольку от них напрямую зависит возможность обучения, дообучения и эксплуатации моделей. В рамках due diligence обычно проверяются условия доступа к вычислительным ресурсам, наличие ограничений на использование сервисов, гарантии доступности (SLA), а также возможность одностороннего прекращения обслуживания со стороны провайдера.

Существенное значение имеют условия об ответственности провайдера за сбои, порядок резервного копирования и восстановления сервисов, а также наличие механизмов оперативного переноса инфраструктуры на альтернативные мощности.



Шермет Курбанов

соруководитель практики интеллектуальной собственности и цифрового права

sll
SL LEGAL

Вопрос инфраструктуры и его критичность сильно зависят от приобретаемого ИИ-бизнеса: от наиболее критичного варианта — (i) случая с собственной ИИ-моделью, и далее в порядке снижения критичности — (ii) случая с адаптацией чужой модели (iii) и случая с использованием чужой недорабатываемой модели (создание архитектуры вокруг чужой модели).

(ii) и (iii) — более частые случаи на текущем M&A рынке, что несколько снижает градус критичности в части инфраструктуры, но все же требует тщательной проверки.

На верхнем уровне при проверке таргета необходимо идентифицировать, условно говоря, внешнюю инфраструктуру (степень зависимости от сторонних поставщиков) и внутреннюю (наличие и достаточность внутренних ресурсов для закрытия вопросов, не закрытых внешней инфраструктурой).

В отношении внешней инфраструктуры в первую очередь необходимо проверить:

- Правомерность использования внешней инфраструктуры для осуществления деятельности (например, с точки зрения локализации данных, наличия надлежащих и стабильных отношений с поставщиком);
- Достаточность для текущей и планируемой деятельности;
- Степень зависимости ИИ-системы от внешнего элемента инфраструктуры (например, чужой ИИ-модели);
- Степень надежности поставщика;
- Возможность перехода в случае необходимости.

В отношении внутренней части инфраструктуры следует проверить как минимум:

- Достаточность для текущей и планируемой деятельности;
- Наличие квалифицированного персонала для работы с внешней и внутренней инфраструктурой и их синхронизацией.

Наибольший риск для ИИ-компании представляет использование сторонней модели в облачном формате. Облачная архитектура модели не позволяет оператору системы независимо дообучать и адаптировать ее на собственных данных, контролировать ее поведение и гарантировать заявленный уровень поддержки (SLA), поскольку все ключевые функции сосредоточены во внешней инфраструктуре.

#ТЕХНИЧЕСКАЯ_ЭКСПЕРТИЗА



Анатолий Земцов

управляющий партнер

dfcenter

В процессе DD важно обратить внимание на следующие технические аспекты в части используемых продавцом инфраструктуры и вычислительных мощностей:

- Наличие в принципе у продавца этих инфраструктуры и мощностей, а также основание такого наличия. Для чего важно изучить техническую документацию об архитектуре ИИ-сервиса (текущей и по плану развития), а в идеале — проанализировать сам ИИ-сервис непосредственно. Также нужно проанализировать документацию об основаниях и объеме прав на использование всех элементов инфраструктуры. Важно понять, какую часть продавец контролирует, обслуживает и за что отвечает сам, а что предоставляется ему третьими лицами.
- Анализ соответствия фактической инфраструктуры декларируемым объемам клиентов / транзакций / иных исчислимых параметров, а также соответствие планам развития. Они могут не соответствовать, что может говорить о возможном маркетинговом преувеличении продавца или об ошибках в технологической части плана масштабирования.
- Техническую актуальность и потенциал развития, масштабирования ИИ-сервиса, с учетом жизненного цикла той базовой технологии или ИИ-модели, которую он использует.
- Степень технологической зависимости ИИ-сервиса продавца от одного стороннего провайдера, одной технологии. Оценить возможность, скорость и по-

тенциальные затраты в случае вынужденной миграции на другой инфраструктурный стек.

- Фактическое местонахождение серверов и иные вопросы, связанные с локализаций данных, расположенных в используемой продавцом инфраструктуре.
- Наличие компетенций и персонала для поддержания, развития и, в случае форс-мажора, экстренного восстановления этой инфраструктуры.



Условия использования инфраструктуры

1. Ключевые области юридического due diligence

- Информация о внешних и внутренних элементах инфраструктуры (серверах, вычислительных мощностях, СХД), используемой для работы ИИ-системы или в связи с ее работой, включая адреса физического расположения всех серверных стоек, СХД, GPU-кластеров, дата-центров, их значимости, достаточности, условиях использования и о поставщиках.
- Документы, подтверждающие правомерность использования каждого элемента инфраструктуры, включая договоры купли-продажи серверного или иного телекоммуникационного оборудования или договоры аренды серверов, а также документы, устанавливающие разграничение эксплуатационной ответственности.
- В отношении элементов внешней инфраструктуры (IaaS) — документы, подтверждающие нахождение всех узлов на территории РФ.
- План мероприятий по обеспечению непрерывности деятельности ИИ-системы на случай блокировки доступа к API модели или облачной инфраструктуре, включая технико-экономическое обоснование возможности миграции сервиса на альтернативную модель.
- Сертификаты соответствия в отношении требуемых уровней защищенности данных в ИИ-системе.
- Наличие у оператора ИИ-системы права на аудит и физическую инспекцию каждого элемента внешней инфраструктуры ИИ-системы и его периодичность.

2. Ключевые red-flag риски

- В SLA с провайдерами облачной (внешней) инфраструктуры отсутствует запрет на миграцию данных за пределы территории РФ, в том числе их «зеркалирование».
- Внешние (арендованные) элементы инфраструктуры используются без договора, либо соответствующие договоры не позволяют использовать инфраструктуру в деятельности компании или существенно ограничивают такую возможность. Может привести к запрету использования внешних элементов инфраструктуры, необходимости поиска альтернатив, взысканию убытков.
- Отсутствие у провайдера инфраструктуры лицензий или сертификатов соответствия требованиям ФСТЭК или ФСБ для обработки данных определенных категорий, а также в отношении программно-аппаратных комплексов, используемых для обучения, инференса модели, если ИИ-система интегрирована в объект КИИ.
- Уголовная ответственность за нарушение режима КИИ (включая нарушение требований по категоризации), если ИИ-система используется на объектах КИИ.

2.1.5 Условия соглашений с конечными пользователями



Считают одним из ключевых вопросов юридической проверки ИИ-компании анализ соглашений с конечными пользователями

#РЕЗУЛЬТАТЫ_ОПРОСОВ

По данным опроса, проведенного в ходе исследования, 27% респондентов в качестве приоритетных областей юридической проверки ИИ-компании отметили вопросы, связанные с условиями соглашений с конечными пользователями ИИ-продукта.

По данным Опроса по аспектам Tech M&A.

Пользовательское соглашение, которое компания заключает с конечными пользователями ИИ-сервиса, особенно в B2C-сегменте, — ключевой инструмент распределения рисков и ответственности между разработчиком (вендором) и потребителями ИИ-сервиса. Такое соглашение позволяет оператору ИИ-системы (владельцу сервиса) в определенной степени ограничить свою ответственность (как гражданско-правовую, так и публичную) за возможные нарушения при использовании ИИ-сервиса конечными пользователями (включая генерацию запрещенного контента, нарушение прав третьих лиц в отношении ОИС и ПДн).

Соглашение с пользователями сервиса может: (i) фиксировать статус вендора как информационного посредника, что позволяет снизить или исключить ее ответственность за нарушение прав третьих лиц в отношении ОИС; (ii) регулировать вопросы использования ОИС и пользовательских данных для целей дообучения моделей и развития ИИ-сервиса; (iii) устанавливать прямые запреты на использование ИИ для противоправных целей, создания запрещенного контента или незаконного использования ПДн; (iv) содержать положения об ограничении ответственности в пределах, допустимых законодательством, в том числе за ущерб, вызванный дефектами работоспособности и иных качественных характеристик сервиса.

В отсутствие такого регулирования на уровне соглашения с конечными пользователями сервиса у компании возрастают риски споров с контрагентами о принадлежности данных, используемых в системе, сопутствующих им регуляторных рисков, а также претензий со стороны регуляторов в связи с нарушением прав широкого круга лиц.

Наличие правильно структурированного соглашения с конечными пользователями позволяет компании создать фундамент для соблюдения ею стандарта должной осмотрительности при эксплуатации и коммерциализации ИИ-сервиса, что может иметь важное процессуальное значение в случае обращения компании за судебной защитой или вступления в процесс, инициированный третьими лицами.

#АНАЛИЗ_РИСКОВ #ПОЛЬЗОВАТЕЛЬСКОЕ_СОГЛАШЕНИЕ

Ключевые риски компании по причине недостаточной проработки условий соглашения с конечными пользователями сервисов связаны со следующими обстоятельствами:

- **В соглашении с пользователями отсутствует запрет на использование противоправного контента при создании запросов к модели, а также на использование сервиса с противоправной целью**,

  в том числе для генерации и распространения вредоносного и запрещенного контента, отсутствуют механизмы блокировки нарушителей. В этом случае вендор не сможет ссылаться на свою осмотрительность и принятие зависящих от него мер для предотвращения инцидента при доказывании своей невиновности, в том числе при подтверждении статуса информационного посредника.

- **В соглашение не включен запрет о недопустимости использования пользователями при формировании запросов ОИС и данных, принадлежащих третьим лицам, без согласия таких лиц**

  Это может повлиять на объем ответственности и степень вины разработчика системы в случае привлечения к ответственности со стороны правообладателей охраняемых объектов.

- **В соглашении не урегулированы вопросы использования контента, включая загружаемые пользователем запросы и данные**,

  в том числе не урегулирована возможность дообучения модели или совершенствования сервиса с использованием таких данных. Это лишает разработчика системы возможности использования ценного массива данных для развития ИИ-сервиса либо создает риск ответственности за противоправное использование таких объектов.

#ПОЛЬЗОВАТЕЛЬСКОЕ_СОГЛАШЕНИЕ



Софья Смирнова

советник M&A
и корпоративной практики

O_2 консалтинг

Пользовательские соглашения ИИ-сервисов должны корректно регулировать порядок использования сервиса, допустимые сценарии эксплуатации модели и распределение рисков между оператором и пользователем. Особое значение имеет наличие ограничений на использование сервиса для противоправных целей, автоматизированного принятия решений или генерации запрещенного контента.

В рамках due diligence также проверяется наличие механизмов обновления пользовательских условий, порядок получения согласий пользователей и корректность положений об ограничении ответственности. Недостаточная проработанность таких условий может привести к спорам с пользователями, претензиям со стороны контрагентов и дополнительным регуляторным рискам.



Шермет Курбанов

соруководитель практики
интеллектуальной
собственности и цифрового
права

sll
SL LEGAL

Пользовательское соглашение с пользователем — это многоцелевой инструмент. В зависимости от конкретной бизнес-модели цели могут быть разными. В качестве наглядного примера у пользовательского соглашения могут быть следующие цели:

- Первый слой — урегулирование отношений с пользователем.
- Второй слой — ограничение частноправовой ответственности. Например, в части интеллектуальной собственности — внедрение положений, указывающих на статус поставщика ИИ-системы как информационного посредника.
- Третий слой — ограничение публично-правовой ответственности. Например, в части включения пользователями в запросы персональных данных, использования или генерации ограниченной или запрещенной к распространению информации.

Нельзя сказать, что все эти «заклинания» работают, но тем не менее они формируют удобную для оператора ИИ-системы отправную точку, которая может существенно снизить или даже устранить некоторые риски.



Алексей Дарков

советник, руководитель практики «Интеллектуальная собственность»

VERBA LEGAL

Условия соглашений с конечными пользователями могут служить важным инструментом защиты ИИ-компании от потенциальных рисков, а потому заслуживают большего внимания. Соглашение может помочь ограничить ответственность компании в случае нарушения пользователем законодательства при использовании ИИ не по назначению или умышленной генерации контента, нарушающего права третьих лиц.

Кроме того, пользовательское соглашение может предусматривать ряд моментов, имеющих значение для коммерческих интересов и развития ИИ-компании: например, положения о сборе данных для обучения или дальнейшей продажи в статистических или маркетинговых целях.

Пользовательское соглашение — ключевой инструмент распределения рисков и ответственности между разработчиком (вендором) и пользователями ИИ-сервиса. Оно позволяет существенно снизить риски споров с контрагентами в отношении данных, используемых в системе, а также претензий со стороны регуляторов в связи с нарушением прав широкого круга лиц.

Условия соглашений с конечными пользователями

1. Ключевые области юридического due diligence

- Текст соглашения с конечными пользователями (его текущей и предыдущих версий и даты изменений, при наличии).
- Порядок информирования пользователей об изменениях условий соглашения и получение их согласия.
- Внутренние документы компании, регулирующие процедуры модерации контента, реагирования на генерацию запрещенных результатов, а также рассмотрения соответствующих жалоб пользователей.
- Образцы уведомлений о недопустимом использовании ИИ-сервиса, которые вендор направлял пользователям (при наличии).
- Описание сценариев использования ИИ, явно запрещенных соглашением (автоматизированные критические решения без участия специалиста, генерация вредоносного кода и т.д.).

2. Ключевые red-flag риски

- Отсутствие соглашения с конечным пользователем. Может привести к требованиям о возмещении убытков / компенсаций без ограничений в связи с использованием сервиса, получаемой пользователем информации, нарушением охраняемых прав третьих лиц.
- Содержание соглашения не соответствует фактическому порядку использования ИИ-системы либо в соглашении не используются механизмы уменьшения / перераспределения ответственности по наиболее актуальным рискам (ОИС, ПДн, ограниченная или запрещенная информация). Может привести к штрафам, взысканию компенсаций.
- Пользовательские данные (включающие охраняемые объекты) используются для дообучения модели, однако в пользовательском соглашении отсутствует согласие пользователя и иные положения, позволяющие оператору системы осуществлять такие действия. Может привести к требованиям о взыскании компенсаций, запрете использования модели.

2.1.6 HR-мотивация ИИ-персонала



Отметили в качестве приоритетных вопросов юридической проверки ИИ-компании условия мотивации ИИ-персонала

#РЕЗУЛЬТАТЫ_ОПРОСОВ

По данным опроса, проведенного в ходе исследования, 10% респондентов в качестве ключевых вопросов юридической проверки ИИ-компании отметили условия мотивации ИИ-персонала

По данным Опроса по аспектам Tech M&A.

В ИИ-сегменте, как и в большинстве бизнесов IT-сферы, экспертиза, опыт и профессиональные компетенции технической команды формируют основные конкурентные преимущества компании и существенную часть ее стоимости. В ИИ-компаниях значительный объем коммерчески ценных знаний сосредоточен не в документированном коде и процессах, а в практическом опыте команды, который далеко не всегда фиксируется и не имеет детальных технических спецификаций, в силу чего его сложно воспроизвести и передать другим лицам.

Покупая ИИ-компанию, приобретатель оплачивает ее будущую способность развивать ИИ-продукт. Эта способность в существенной мере связана с фактором сохранения текущей ИИ-команды на продолжительное время, достаточное для реализации стратегических целей бизнеса. Уход ключевых работников после сделки, особенно в случае перехода ключевых специалистов к конкурентам, может привести к утрате компанией стратегических возможностей и тем самым существенно снизить ее стоимость. Поэтому в контексте сделки M&A **команда ИИ-персонала сама по себе является ценным активом**, а в ряде случаев, например в проектах acquihiring, — целевым объектом приобретения.

По мере роста глубины и сложности отечественных ИИ-продуктов потребность в уникальных специалистах будет только расти. На фоне острого дефицита ИИ-персонала замена ушедших сотрудников является длительной и затратной процедурой. Поэтому в условиях жесткой конкуренции за ИИ-компетенции на рынке труда компаниям важно обеспечить условия, при которых команда будет заинтересована остаться в этом активе и продолжить его развитие.

Поэтому наличие в ИИ-компании программы долгосрочной мотивации ИТ- и, в особенности, узкоспециализированного ИИ-персонала (ML-инженеры, специалисты в области данных), обеспечивающего создание, развитие и поддержку основных ИИ-систем и продуктов бизнеса, должно стать обязательным этапом прединвестиционного due diligence. В рамках юридической и кадровой проверки необходимо проанализировать текущие и планируемые условия как финансовой, так и нефинансовой мотивации ключевого ИИ-персонала, непосредственно связанного с разработкой и поддержанием ИИ-решений, а также влияние вопросов корпоративной культуры приобретателя на их решение остаться в компании.

#АНАЛИЗ_РИСКОВ #МОТИВАЦИЯ_ИИ_ПЕРСОНАЛА

Неблагоприятные последствия, связанные с отсутствием в компании сбалансированной программы долгосрочной мотивации ИИ-специалистов, обусловлены следующими факторами:

- **В компании отсутствует сбалансированная программа долгосрочной мотивации ИИ-специалистов**

  Это может привести к увольнению всей команды или единичных ключевых ИИ-специалистов после закрытия сделки, в том числе их переходу к конкурентам, предложившим более привлекательные условия. В результате этого компания может утратить актив в виде интеллектуального капитала и конкурентные преимущества, контроль над конфиденциальной информацией и внутренним ноу-хау в сфере ИИ, а также часть клиентской базы, что может существенно ослабить ее рыночную позицию.

- **Невозможность адекватной технической поддержки или ее существенное усложнение или удорожание**,

  если уникальные «носители» специальных знаний покинули компанию после сделки. Оставшиеся или новые сотрудники не всегда способны быстро воспроизвести исторические методы дообучения модели, настройки гиперпараметров или устранить иные ошибки в работе ИИ-системы, объективно оценить точность и безопасность модели. Это может способствовать быстрой деградации продукта и репутационным рискам.

- **Неконтролируемое снижение качества работы ИИ-системы и основанных на ней активов**

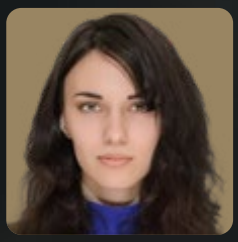
  Без ключевых ИИ-специалистов, непосредственно участвующих в процессе дообучения и адаптации модели, приобретателю будет сложно самостоятельно установить причину возникновения инцидентов и атрибутировать ответственность за исторические риски. Это может привести к репутационным потерям и штрафным санкциям перед заказчиками и пользователями продукта.

- **Утрата контроля над разработками, процесс которых не был корректно документирован**

  В ИТ-бизнесах многие важные процессы традиционно плохо документируются, в сфере ИИ — многие процессы и опыт в принципе не фиксируются или это происходит несвоевременно, большой объем коммерчески значимой информации существует в форме «знаний» разработчиков, которые не формализуются в качестве секретов производства. Утрата истории экспериментов и воспроизводимости результатов ИИ-системы может сделать невозможным возврат (откат) к предыдущим стабильным версиям модели. Если метрики и конфигурации экспериментов хранятся только в локальных средах разработки ушедших ИИ-специалистов и не включены в систему контроля версий компании, — этот риск не может быть восполним простым «переписыванием кода» или заменой одного специалиста другим.

В ИИ-компаниях значительный объем коммерчески ценных знаний сосредоточен не в документированном коде, а в практическом опыте команды, который далеко не всегда фиксируется, не имеет детальных технических спецификаций и «привязан» к его носителям.

#МОТИВАЦИЯ_ИИ_ПЕРСОНАЛА



Анастасия Нерчинская

Далеко не все специалисты, участвующие в продуктовой разработке, могут ответить на вопрос, почему конкретная архитектура ИИ-модели показала превосходство на определенном наборе данных, какие трансформации обучающих данных (аугментация, фильтрация, разметка) оказались решающими для целевых метрик системы, как выстроен весь цикл экспериментов, который привел к рабочему решению. Эти знания неявны, они накапливаются эмпирически и привязаны к их «носителям», то есть к конкретным работникам. Их уход из компании после закрытия сделки может привести к тому, что новый владелец бизнеса, даже имеющий собственную ИИ-команду, не сможет быстро воспроизвести текущий уровень качества, адаптировать модель к дрейфу данных, поддерживать точность и безопасность ответов системы на целевом уровне. Дообучение моделей без понимания ее экспериментальной логики в рамках конкретной системы может привести к непредсказуемым результатам. Поэтому при приобретении ИИ-компании вопросы мотивации ИИ-команды важны и требуют особого внимания.



Илья Булгаков

советник

DÉNUO

Пока что процент респондентов, указывающих на важность мотивационной программы для ключевых сотрудников, достаточно мал. Я это связываю с двумя факторами.

Во-первых, отсутствие механизмов для создания полноценной мотивационной программы в частных компаниях в России (структурирование понятной опционной программы с понятными условиями вестинга, клифа).

Во-вторых, пока что в России мало проектов в сфере ИИ, которые бы требовали очень квалифицированных кадров (научных сотрудников, людей с опытом создания ИИ-продуктов). Обычно для создания продуктов привлекается «классическая» команда из разработчиков, devops, дизайнеров, и не всегда даже в команде есть ML-инженер. Это связано с тем, что в России зачастую компании строят свои бизнесы вокруг какой-то уже выведенной на рынок ИИ-модели или делают минимальные услушения за счет RAG. По сути эта работа может выполняться квалифицированными бэкенд-разработчиками с опытом в построении LLM-pipelines, что не требует привлечения сотрудников с научными степенями в области ИИ. Соответственно, мотивации в привлечении и удержании особо ценных сотрудников пока в российских компаниях в сфере ИИ нет или она может закрываться через механизмы бонусов и высоких зарплат.



Алексей Дарков

советник, руководитель практики «Интеллектуальная собственность»

VERBA LEGAL

Этот пункт часто игнорируют, хотя именно команда — ключевой актив ИИ-компании. С одной стороны, ключевые сотрудники могут по ряду причин покинуть место работы, если не будут предложены новые условия мотивации. Кроме того, по оценке Минцифры, в 2024 г. нехватка IT-специалистов достигала 700 тыс. человек, а к 2025 г. может вырасти до 1 млн[40], что наводит на мысли о важности создания и сохранения инновационного «человеческого» потенциала.

Условие не стоит игнорировать и по другим причинам. Ключевые сотрудники могут влиять на принятие определенных решений и, наоборот, получать особые условия по бонусам, рассчитываемым от показателей бизнеса.

В обоих случаях условия о сохранении команды либо о безболезненной смене относятся к решению бизнеса. Однако юридически указанные аспекты не стоит упускать, так как они напрямую могут влиять на условия сделки.

[40] https://rb.ru/news/it-specialists-million/



Софья Смирнова

советник M&A
и корпоративной практики

O_2 консалтинг

Наличие адекватной мотивационной программы для ключевых работников. Для ИИ-компаний существенное значение имеет удержание ключевых разработчиков, ML-инженеров и исследователей, поскольку именно их экспертиза зачастую определяет ценность бизнеса.

В рамках due diligence, помимо базовой проверки корректного оформления прав на результаты интеллектуальной деятельности работников, мы также проверяем наличие опционных программ, механизмов долгосрочной мотивации. Отдельное внимание уделяется рискам, связанным с уходом ключевых сотрудников: наличию соглашений о конфиденциальности, неконкуренции (если применимо) и надлежащему оформлению служебных произведений, разработок и ноу-хау.

Отсутствие таких механизмов может привести к утрате контроля над критическими элементами ИИ-продукта или существенному снижению стоимости компании. В ИИ-проектах, где ключевую ценность носит именно команда и бизнес-результат еще не в полной мере реализован (для чего и привлекаются внешние инвестиции), особенно важно предложить всесторонне продуманную систему мотивации ключевого персонала (включая good leaver / bad leaver сценарии).

Покупая ИИ-компанию, приобретатель оплачивает ее будущую способность развивать ИИ-продукт. Эта способность в существенной мере связана с фактором сохранения текущего ИИ-персонала на продолжительное время, достаточное для реализации стратегических целей бизнеса.

Условия мотивации ИИ-команды

1. Ключевые области юридического due diligence

- Информация о системе бонусов (премий), выплачиваемых работникам, участвующим в разработке и эксплуатации ИИ-систем, на регулярной основе или в зависимости от достигнутых результатов работы.
- Информация о выплатах, осуществляемых работникам, участвующим в разработке и эксплуатации ИИ-систем в дополнение к обязательным, о текущих и планируемых мотивационных и опционных программах в отношении таких работников, а также о соглашениях, заключенных компанией с третьими лицами в пользу своих работников (например, медицинское страхование, страхование жизни и т. д.).
- Действующие трудовые договоры и должностные инструкции ключевых работников, связанных с проектированием и поддержанием ИИ-систем.

2. Ключевые red-flag риски

- В компании отсутствует мотивационная программа для ключевых ИИ-работников, что повышает вероятность риска их ухода из бизнеса после закрытия сделки.
- Текущая программа долевого участия работников в капитале компании (опционная программа) сложно структурирована, в нее включены дополнительные компании (например, в качестве операторов, выполняющих функцию держателя зарезервированной опционной доли), которые приобретатель может не быть готов включить в контур сделки, особенно в случае, если таким оператором выступает ЗПИФ или иностранная компания.
- В мотивационную программу включены условия выплат, предполагающие, что они должны быть осуществлены только при приобретении компании, но не в зависимости от результатов дальнейшего развития продукта.

2.1.7 Иные типы рисков ИИ-систем

Выше были отмечены наиболее распространенные **юридические риски**, связанные с созданием, эксплуатацией и коммерциализацией ИИ-систем. Однако при использовании решений на основе ИИ-технологий могут проявляться и другие типы рисков[41]. Чаще всего к ним относят следующие категории.

Социально-этические риски

- **Алгоритмическая предвзятость (смещение) модели**, в результате чего в ее работе появляется т. н. смещение (bias) — выдача результатов, дискриминирующих определенные группы лиц по различным признакам.

[41] Более подробно возможные риски использования базовой модели при создании и эксплуатации ИИ-системы рассмотрены в разделе 1 главы 3 исследования «Периметр ключевых активов ИИ-компании в контексте M&A»

#АНАЛИЗ_РИСКОВ



Софья Смирнова

советник M&A
и корпоративной практики

O_2 консалтинг

Выдача генеративных ML-моделей может быть дискриминирующей (модели воспроизводят предвзятость обучающих данных, этот феномен называется алгоритмическая предвзятость), за что ответственность, согласно общим принципам, должна быть возложена на оператора системы. Требовать от продавца актива отсутствия такой предвзятости, равно как и гарантировать это технически невозможно. Поэтому на данном этапе развития технологии кажется справедливым запрашивать заверения о наличии систем мониторинга и процедур переобучения на «очищенных» от дискриминации (в случае ее обнаружения) данных либо, в зависимости от структуры сделки, возлагать данные обязательства на продавца.

- **Генерация моделью запрещенных результатов, манипуляция общественным мнением и дезинформация пользователей**

  путем создания контента, нарушающего нормы морали, синтетического имитационного контента, способного вводить в заблуждение (например, «дипфейков»), в том числе имитирующего деятельность человека в тех сферах, где требуется его личное участие, иного нежелательного контента.

- **Автономия и отсутствие контроля при принятии решений**

  В ряде случаев законодательство требует валидации человеком ответов автоматизированных систем, к которым в полной мере можно отнести многие ИИ-системы.

Указанные риски негативно влияют на общественные блага и морально-этические нормы. Даже если причина этих рисков лежит в технической плоскости — их последствия носят выраженный социальный характер.

Ключевые области проверки

- Анализ корпоративной политики или иного документа компании, регулирующего вопросы этики при создании и использовании ИИ-систем и сервисов.
- Комплекс мер, реализуемых компанией направленных на снижение степени предвзятости ответов используемых моделей.
- Наличие контура «человек в принятии решений», в рамках которого ответы модели по критически значимым аспектам, включая такие, которые влекут юридические последствия для пользователя, проверяются человеком.
- Проверка ИИ-системы в рамках особого вида due diligence при участии комплексной рабочей группы на предмет выявления дискриминационных паттернов и склонности к генерации запрещенного или вредоносного контента.

Материализация таких рисков может привести к высоким репутационным рискам ИИ-продукта, требованиям пользователей о возмещении ущерба и компенсации морального вреда, уголовной ответственности за распространение запрещенной информации.

Архитектурно-технологические риски

- **Снижение точности ответов модели,**

  неизбежно появляющиеся с течением времени. Это следствие проявления ее архитектурного свойства — т. н. дрифта данных или концепции (data drift / concept drift).

#ТЕХНИЧЕСКАЯ_ЭКСПЕРТИЗА



Анатолий Земцов

управляющий партнер

dfcenter

Степень дрифта можно определить без доступа к обучающим датасетам через black-box-оценку: тестирование модели на независимом контрольном наборе, сравнение текущих метрик с историческими (если они зафиксированы), анализ изменения распределения входных данных и ответов. Это позволяет зафиксировать факт и масштаб ухудшения качества, но не причины.

Установить момент, когда ухудшение стало следствием действий интегратора, возможно только при наличии журналирования, версионности весов и конфигураций, истории релизов и baseline-метрик на конкретные даты. Без этих артефактов причинно-следственная связь доказуема лишь вероятностно.

- **Необъяснимость ответов модели (explainability) —**

  отсутствие прозрачного механизма, обосновывающего принятие моделью конкретных решений. Это свойство технологии может быть критично для создания прикладных решений в социально чувствительных областях, например, здравоохранении, финансах, транспорте.

- **Генерация «галлюцинаций» —**

  формирование ИИ-системой убедительных ответов, содержащих ложные данные. Например, несуществующие биографические сведения, судебные дела или некорректную медицинскую информацию.

- **Непрозрачность —**

  пользователи не знают, что взаимодействуют с ИИ-системой.

Технологические риски происходят из фундаментальных ограничений архитектуры моделей как инженерных систем и ее внутренних свойств и проявляются даже при отсутствии внешнего злонамеренного воздействия на данные, а также вне прямого социального контекста. Технологические риски могут быть предпосылками этических рисков.

Ключевые области проверки

- Анализ политики или иного документа компании, регламентирующего процедуру фиксации и мониторинга дрейфа используемых ИИ-моделей и точности их ответов, а также меры реагирования на снижение производительности и точности моделей.
- Комплекс мер, фактически реализуемых компанией, направленных на смягчение дрейфа моделей, используемых в коммерческих продуктах, «галлюцинаций», предвзятости ответов (механизмы дообучения, промпт-инжениринг, управление контекстом через RAG на основе этичных источников данных, фильтрация, использование моделей-модераторов, регулирование гиперпараметров и т. п.).
- Аудит качества данных — степень зашумления, полноты, репрезентативности, дефектов разметки.

Материализация таких рисков может привести к быстрой деградации моделей и, соответветственно, качеству ИИ-сервиса, что в конечном итоге приведет к снижению стоимости бизнеса.

ИБ-риски

- **Компрометация логики работы ИИ-системы через вредоносные запросы (промпт-инъекции)**,

  приводящая к обходу внутренних политик безопасности.

- **Атаки на ИИ-модель —**

  умышленное искажение входных данных в ИИ-систему, которые заставляют модель ошибаться, вредоносное «отравление» обучающих данных.

Ключевые области проверки

- Результаты пентестов и аудита безопасности компонентов ИИ-системы с учетом применимых категорий угроз.
- Сертификаты регуляторов, если ИИ-система обрабатывает критически значимую информацию или планируется к интеграции в объекты КИИ.
- Модель ИИ-угроз ИИ-системы и комплекс мер, применяемых в компании, направленных на защиту от специфических ИИ-атак (защита от промпт-инъекций, мониторинг аномальной активности доступа к системе).

ИБ-риски связаны с обработкой информации на протяжении всего жизненного цикла ИИ-системы, где центральный объект атаки или непреднамеренного раскрытия — сами данные (их конфиденциальность, целостность, доступность). Точки уязвимости находятся непосредственно в слое данных, где и происходит инцидент утечки, незаконного изменения, несанкционированного извлечения.

Материализация таких рисков может привести к крупным утечкам данных, в том числе чувствительных, компрометации конфиденциальной информации, получению ИИ-системой несанкционированного управления, и связанным с этими рисками штрафным санкциям, а также уголовной ответственности.

На практике границы между этими рисками и причинами их возникновения стираются. Компрометация данных (ИБ-риск) может вызывать сбой в работе модели (технологический риск), который, в свою очередь, может привести к несправедливым решениям (социально-этический риск). Поэтому категоризация не устраняет **необходимости комплексного управления рисками, где три группы рассматриваются как единый ландшафт угроз**.

#УПРАВЛЕНИЕ_РИСКАМИ



Софья Смирнова

советник M&A
и корпоративной практики

O_2 консалтинг

Создание ИИ-сервиса требует управления новыми рисками, в том числе имманентными природе нейросетей. Лучшей практикой будет являться принятие следующих защитных мер.

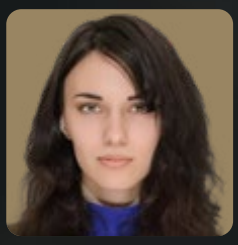
1. **Аудит данных.** ИИ учится на данных и воспроизводит их искажения. Если в обучающих данных есть перекосы (например, гендерные), модель будет их повторять. Например, HR-модель училась на данных, где руководящие должности чаще занимают мужчины, она может дискриминировать женщин при скоринге резюме. Разумно гарантировать отсутствие дискриминации во всех случаях может быть невозможно, но необходимо предпринять надлежащие усилия. Для корректного скрапинга в Интернете поможет следующее: не обходить технические барьеры площадок в Интернете, не извлекать существенную часть, избегать платформ с ПДн.
2. **Защита от промпт-инъекций.** Пользователь может специальными запросами «обмануть» ИИ и получить закрытую информацию. Обычные антивирусы тут не помогут — нужны фильтры (guardrails), блокирующие подозрительные запросы до их обработки моделью.
3. **Мониторинг качества и объяснимости.** В силу вероятностной природы LLM она принципиально не всегда способна объяснить результат генерации и со временем качество ее ответов падает («дрифт / дрейф данных»), а логика ее решений становится запутаннее. Поэтому важно вести логи рассуждений модели, а юридически значимые решения (например, отклонение резюме) должен проверять человек.
4. **Безопасность данных.** Основные риски утечки: данные клиента попадают в облако провайдера и всплывают в ответах другим; персональные данные уходят за рубеж в нарушение закона о локализации (ФЗ-152); модель может «вычислить» конкретного человека из якобы обезличенных данных. Все это требует постоянной интеллектуальной фильтрации на входе и шифрования хранимых данных. Маскировка подобного контента должна происходить постоянно и интеллектуализированно.

5. **Маркировка сгенерированного контента.** Если сервис создает изображения, видео или аудио, их нужно автоматически помечать как сгенерированные. Пока это не обязательно по закону, но, скорее всего, станет — и уже сейчас снижает репутационные риски (см. законопроект об ИИ ниже).
6. **Независимость от конкретной LLM.** Инфраструктуру лучше строить так, чтобы «мозг» (LLM) можно было заменить с минимальными затратами — на случай ужесточения регулирования или появления лучших решений.
7. **Документирование затрат и защита коммерческой тайны.** Для обоснования смежного права на базы данных, собранные для функционирования RAG, необходимо обосновать понесенные затраты на их создание и доказать, что они существенные. Инженерные решения в рамках базы могут охраняться как ноу-хау или как объект авторского права (в составе базы данных как объекта), оба режима требуют внимательной документарной работы.
8. **Локализация.** Тенденции законодательного регулирования тяготеют к тому, что рынок будет принадлежать только доверенным ИИ-продуктам, LLM в составе которых прошли специальную сертификацию ФСТЭК и ФСБ. Несмотря на отсутствие прямых ограничений для B2B-использования, B2G и B2C-рынок будет локализовываться, о чем свидетельствует проект ФЗ об ИИ, сформированный Минцифры. Отдельным вопросом является применение к ИИ-сервисам «закона Яровой». Представляется, что в настоящий момент он может быть не применим, но п. 10.3 проекта ФЗ об ИИ будет применять его к ИИ-сервисам с количеством пользователей более 500 тыс. в сутки.

Поскольку юридические вопросы в рамках слоя базовой модели неподконтрольны третьим лицам, в том числе операторам сторонних ИИ-систем, управление рисками при создании и эксплуатации прикладных ИИ-решений целесообразно выстраивать через:

- Мониторинг объективных метрик поведения модели (дрейф и точность модели, алгоритмическая предвзятость, безопасность ответов и т. п.).
- Фиксацию динамики этих метрик с момента начала использования модели продавцом (разработчиком ИИ-системы).
- Распределение ответственности в рамках сделки на основе того, какие метрики и с какого момента продавец мог отслеживать.

#УПРАВЛЕНИЕ_РИСКАМИ



Анастасия Нерчинская

С самого начала эксплуатации ИИ-системы ее разработчик начинает влиять на ряд важных параметров модели, интегрированной и адаптированной в конечный продукт. Оператор системы, основанной на сторонней модели, не контролировал процесс предобучения базовой модели, как и все последующие циклы ее дообучения, если сам не принимал в них участие. Более того, не он (как и не разработчик модели) создал ИИ-технологию, поэтому не может отвечать и за риски, связанные с ее архитектурными свойствами.

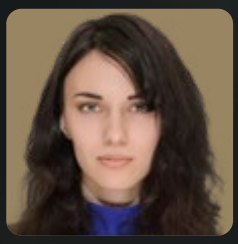
Но разработчик ИИ-системы несет ответственность за собственные действия в сфере своего влияния, которая довольно широка — выбор модели, ее версии и конфигураций, слой данных, включая дообучение модели, если оно осуществлялось под его контролем, процедуры тестирования и валидации, мониторинга, логирования, реагирования на инциденты, процесс наблюдения за динамикой метрик функционирования системы и многое другое.

Если в ИИ-компании не внедрены процедуры мониторинга ключевых параметров поведения модели и не реализованы необходимые практики, продавцу будет гораздо сложнее ответить на соответствующие вопросы покупателя, распределить риски (юридические, технические, этические), обеспечить качественное структурирование сделки на своей стороне. ИИ-комплаенс имеет важное практическое значение. Используя данные журналирования инцидентов, логирования, результаты тестирования и валидации, продавец сможет обосновать разграничение между собственной сферой контроля и внешними факторами влияния на поведение модели, за которые он не отвечает.

Покупателю, в свою очередь, без такой информации придется восстанавливать факты и выстраивать процессы «с нуля» с помощью дорогостоящего ретроспективного анализа, что может потребовать дисконта к цене.

2.2 Подходы к организации due diligence ИИ-компаний

Юридическая проверка активов, в основе которых лежат ИИ-системы, требует существенной адаптации традиционной методологии due diligence. Это обусловлено спецификой проверяемого объекта, включающего ИИ-технологию помимо привычных аспектов проверки (ПО, данные, регуляторные вопросы). ИИ-компонента предопределяет исключительно **высокую степень асимметрии информации** в сравнении с другими типами проверяемых активов, что крайне **сужает объективные пределы ее анализа**. Это порождает разрыв между ожидаемой юристами степенью полноты проверки и объективной возможностью ее проведения. При организации юридического due diligence ИИ-компании следует учитывать эту особенность, чтобы такая проверка была эффективной.



Анастасия Нерчинская

В рамках due diligence ИИ-системы проверить юридическую чистоту всех значимых вопросов, относящихся к ИИ, — заведомо невыполнимая задача. Это связано с особенностями ИИ-технологии, риски которой понятны, но многие из них принципиально не проверяемы либо не имеют правильного «носителя» среди участников сделки, кому можно было бы адресовать ответственность за такой риск. Фактически это означает, что все такие вопросы относятся к зоне предпринимательского риска участников сделки.

В рамках due diligence разработчик ИИ-системы имеет реальную возможность предоставить далеко не все документы и информацию по запросу покупателя. Информация по вопросам, связанным с предобучением и дообучением модели, которые осуществлял разработчик модели,некоторым вопросам управления этическими, техническими, а также ИБ-рисками, у разработчика ИИ-системы просто отсутствует. Такие сведения в абсолютном большинстве случаев носят закрытый характер и принадлежат третьим лицам, в первую очередь разработчику модели.

Информация по этим вопросам, которой располагает ИИ-компания, скорее всего, доступна для всеобщего сведения, в том числе для гипотетических покупателей (например, опубликованная разработчиком модели документация, связанная с особенностями и ограничениями использования модели).



Артем Евсеев

советник практики
интеллектуальной
собственности

ЭБР
Юридическая
Компания

При проведении юридической проверки ИИ-продуктов всегда важно понимать, что такая проверка чисто практически имеет значительные ограничения в отличие от проверки классических программных продуктов.

Если мы говорим про ПО, то его достаточно легко разбить на составные элементы (ядро, модули, надстройки, библиотеки) и для каждого из таких элементов провести проверку. Например, если компонент является сторонним, то в большей части случаев достаточно убедиться в соблюдении лицензионных условий на такой компонент. Если компонент представляет собой собственную разработку, то необходимо изучить, как были оформлены отношения с работниками, выплачивалось ли им авторское вознаграждение и пр.

С юридической точки зрения проверка ИИ-решений особо не отличается от проверки обычного ПО. Однако, как и в любом вопросе, дьявол кроется в деталях. ИИ-решения, которые являются предметом M&A сделок, как правило, разработаны на основе имеющихся ИИ-моделей. Казалось бы, ничего сложного, нужно просто проверить чистоту прав на эту ИИ-модель, то есть поступить так же, как и в случае с классическим ПО. Но не все так просто, к сожалению.

ИИ-модель не является классическим ПО. Это не просто компьютерный алгоритм с определенными функциями и параметрами. Это результат гигантского количества математических преобразований на основе большого объема данных, загруженных в ИИ-модель в ходе ее обучения. И вот здесь и заложена ключевая проблема — никто не может убедиться на все 100%, что модель была обучена на данных, которые были получены законным образом. В ходе сделки мы не можем проверить, были ли в модель загружены для обучения персональные данные, были ли получены согласия субъектов данных на их обработку, использовались ли при обучении объекты интеллектуальных прав, дали ли правообладатели свое согласие на такое использование и пр.

Все эти риски берут на себя участники сделки. Продавец сервиса или, грубо говоря, надстройки над ИИ-моделью в большей части случаев никак не может полностью проверить, на каких данных обучалась ИИ-модель, и повлиять на изменение таких датасетов.

Естественной реакцией любого юриста на стороне покупателя будет сразу включить в сделку условия о возмещении потерь и / или заверения об обстоятельствах. Но в таком случае продавец просто не захочет брать на себя такие чрезмерные риски.

Поэтому правильным может быть поиск разумного компромисса, потому что в противном случае ни одна M&A сделка в сфере ИИ вряд ли сможет состояться.

Что следует учитывать при организации юридического DD ИИ-системы

Методологию юридического due diligence ИИ-активов следует выстраивать исходя из:

- **Четкого разделения областей проверки**

  на сферу, где анализ принципиально возможен, и зону объективной неопределенности.

- **Отказа от запроса излишней информации**

  и заведомо неисполнимых требований о полной верификации объектов, связанных с зоной ответственности разработчика базовой модели.

- **Формата использования модели (закрытый или открытый)**

  Чем больше артефактов модели и информации о них раскрыто и доступно для скачивания, тем шире могут быть объем и глубина проверки (как юридической, так и технической), так как больше аспектов может быть объективно проанализировано по существу.

- **Юрисдикции происхождения модели**

  Использование зарубежной ИИ-модели делает прикладное ИИ-решение уязвимым для множества сценариев. Поэтому акцент проверки смещается в сторону анализа принципиальной допустимости ее использования, санкционных рисков и возможной блокировки доступа к модели и ее обновлениям. В этом случае может быть необходимо привлечение иностранных консультантов, практикующих в соответствующей юрисдикции.

- **Активного взаимодействия с техническими экспертами**

  в процессе юридической проверки ИИ-активов и использования результатов технического аудита.

- **Учета данных из других сфер компетенции**,

  связанных с ИИ, в том числе информации из систем мониторинга параметров ИИ-системы, если соответствующие процедуры были внедрены разработчиком системы.

- **Назначения и функциональной роли ИИ-продукта**

  в бизнесе приобретаемой компании и покупателя. Если продукт используется для поддержки ключевых функций бэк-офиса, автоматизации внутренних процессов, которые напрямую не влияют на оценку компании, степень и глубина проверки может быть ниже.

- **Отраслевой специфики применения ИИ-решения**

  Сфера внедрения ИИ-решения (например, банковский сектор, медицина или промышленность) может требовать анализа дополнительных вопросов, связанных с эксплуатацией ИИ-системы.

> **ИИ-компонента предопределяет исключительно высокую степень асимметрии информации в сравнении с другими типами проверяемых активов, что крайне сужает объективные пределы ее анализа.**



Шермет Курбанов

соруководитель практики интеллектуальной собственности и цифрового права

sll
SL LEGAL

@SLLEGAL →

Юридический due diligence ИИ-активов целесообразно проводить поэтапно, так, чтобы каждый следующий уровень проверки углублял анализ. Ключевыми являются три этапа:

1. **Определение юрисдикций.** Ключевой особенностью ИИ-активов является их трансграничный характер: они могут создаваться, дообучаться и использоваться в разных юрисдикциях. Поэтому отправной точкой проверки является определение всех правовых систем, требования которых подлежат оценке: как российское регулирование, так и применимое зарубежное.
2. **Базовый анализ.** На втором этапе анализа ИИ-активы требуют проведения традиционных для ПО процедур проверки, включая анализ титула на ПО, технический due diligence, оценку безопасности и соответствия требованиям к защите информации.
3. **Расширенная экспертиза.** Этот этап проверки пересекается с предыдущим и концентрируется на уникальных особенностях ИИ, которые по-новому раскрывают известные правовые проблемы и формируют принципиально иные риски, требующие специальной проверки.



Владислав Лазуткин

старший юрист

ORION

Каким образом анализировать риски использования ИИ (включая генеративный) в сделках Tech M&A — зависит от значения использования ИИ, так как он может выступать основным продуктом / его отдельным компонентом либо иметь второстепенное значение, например, использоваться бэк-офисом.

Массив данных необходимо распределить по категориям, так как обработка различных типов данных регулируется по-разному (персональные данные, сведения из баз данных, авторские материалы и т. п.).

Категории, источники, потоки данных и способы их использования предопределяют и юридический анализ рисков, связанных с их обработкой.

С учетом трансграничной фрагментации бизнеса приходится обращать внимание не только на различные подходы к вопросу о правах на продукты генерации ИИ в РФ, но и на преобладающие подходы по аналогичным вопросам в иных странах, в которых целевая компания имеет присутствие.



Анна Максименко

партнер

KKMP LEGAL

На сегодняшний день практически каждый второй бизнес использует ИИ в бизнес-процессах. Это могут быть как сторонние системы ИИ, так и собственные; использование ИИ может быть как вспомогательным инструментом, так и решением, которое интегрировано во все бизнес-процессы: от разработки модели и обучения на данных до работы с пользовательской информацией и интеграции результатов в ключевые процессы компании. Для нашей команды анализ использования ИИ приобретаемым бизнесом стал обязательной частью юридической проверки в сделках Tech M&A, поскольку на каждом этапе использования ИИ могут возникать нарушения, способные привести к уничтожению модели, блокировке бизнес-процессов, спорам с правообладателями. Каждое из нарушений может привести к репутационным, имущественным потерям (включая штрафы, компенсацию убытков, расходы на консультантов, финансовые потери в результате необходимости перестройки бизнес-процессов), ответственности менеджмента. Степень существенности рисков зависит от роли, которую ИИ занимает в бизнесе компании, и от самой ИИ-модели (например, генеративный ИИ имеет более высокий риск-профиль).

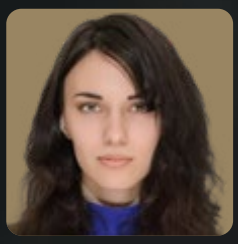
Результаты юридической проверки ИИ-активов приобретаемой компании могут напрямую влиять как на покупную цену, так и на содержание гарантий и заверений в документации по сделке.

Вопросы ИИ, принципиально проверяемые в рамках юридического due diligence, сосредоточены вокруг правомочий и условий использования сторонней базовой модели, правомерности использования данных для ее адаптации и эксплуатации, за исключением предобучающих датасетов модели, а также вопросов open source ПО, использование которого очень распространено при создании ИИ-продуктов.

Предварительная оценка объема проверки

Для целей эффективного распределения ресурсов при проведении юридической проверки ИИ-системы и составлении запроса компании на предоставление документов, следует адекватно оценить объем сведений, которыми располагает компания. В первую очередь (например, в рамках установочного звонка с технической командой компании), следует установить, располагает ли она информацией в отношении:

- **Используемой модели** — тип, версия, источник, количество используемых моделей, условия их совместимости (если их несколько), доступные артефакты (веса, инференс, конфигурации, иное), условия и ограничения использования, включая связанные с масштабированием продукта.
- **Предобучающих датасетов** — происхождение данных, наличие разрешительных документов (лицензий, согласий), наличие прямого доступа к датасетам, информация о гарантиях разработчика модели в отношении предобучающих данных, сведения, раскрытые разработчиком модели о предобучающих данных.
- **Прочих элементов, используемых поверх модели**, в том числе элементов традиционного ИТ-стека ИИ-решения, включая функциональное и инструментарное ПО, системные промпты, реляционные и векторные базы данных, описание архитектуры, техническую документацию.
- **Данных, используемых при создании и эксплуатации ИИ-системы** — форматы адаптации модели в ИИ-системе, источники дообучающих данных (если модель адаптируется путем дообучения) и данных, обогащающих контекст модели без ее изменения, методов формирования датасетов, контроля за процессом подготовки данных (разметка, очистка, обезличивание т. п.), разрешительная документация.
- **Используемой инфраструктуры** — вычислительные мощности (GPU), средства хранения и обработки данных, а также условия их предоставления (договоры с провайдерами, лицензионные соглашения).



Анастасия Нерчинская

Прежде чем направлять в таргет слишком детальный запрос в отношении ИИ-аспектов и просить компанию потратить ресурс на ее получение, нужно определить, проверяем ли соответствующий риск в принципе и что его проверка даст в конечном итоге. Допустим, что покупателю будет предоставлен прямой доступ к огромному предобучающему датасету модели с возможностью его white-box тестирования. Каким образом он проверит, получил ли создатель этого датасета или разработчик модели согласия у владельцев соответствующих данных? А главное – сможет ли он, в случае обнаружения в этих датасетах охраняемого контента третьих лиц, убедить разработчика модели удалить ее или полностью переобучить, чтобы «вылечить» риски для целей свой сделки?

Стандарт должной осмотрительности

При приобретении ИИ-активов приобретателю важно обеспечить соблюдение стандарта должной осмотрительности, если он планирует использовать заверения продавца в качестве средства распределения ИИ-рисков. Однако если говорить о сделке M&A с бизнесом на основе ИИ-системы, в которую интегрирована сторонняя модель (а таких случаев абсолютное большинство), вопрос стандарта осмотрительности довольно сложен.

С одной стороны, очевидно, что ИИ-технология заведомо сопряжена с высокими рисками, вероятность выявления которых велика, а возможности их реальной митигации практически отсутствуют. С другой — покупателю в случае спора по недостоверным заверениям необходимо обосновать, что он предпринял все зависящие от него меры, чтобы собрать необходимую информацию, а если таковая не была ему предоставлена — доказать это обстоятельство, как и то, что у него отсутствовала самостоятельная возможность получить необходимые сведения.

> **Стандарт осмотрительности в сделках ИИ «сталкивается» с объективным пределом, за которым риски принимаются покупателем либо распределяются на контрагента по сделке — если продавец согласится принять излишние риски — путем соответствующих договорных механизмов.**

В связи с этим особое значение приобретает проверка самим покупателем всех открытых источников значимой информации в отношении используемой ИИ-технологии. Зачастую для этого достаточно только знать название и версию используемой ИИ-модели. Поэтому если продавец или компания не предоставят никакой иной информации в отношении модели, покупатель не сможет просто так ссылаться на это обстоятельство при доказывании своей осмотрительности. Важно помнить, что абсолютное большинство сведений в отношении ИИ-технологий доступны для широкого круга лиц, за редким исключением использования дорогих кастомизированных on-prem моделей. Такую информацию может публиковать непосредственно разработчик модели, в том числе в отношении закрытых (проприетарных) моделей, вопрос лишь в объеме сведений и доступных для распространения артефактов.

Некоторые модели, распространяемые в формате open source, могут полностью раскрывать состав датасетов, на которых предобучалась базовая модель. Эти данные доступны также и для покупателя. В этом случае он сможет проверить такой датасет в формате white-box, имея прямой доступ к нему.

Это может иметь значение в ситуации, когда покупатель, проверив такой датасет средствами технической экспертизы и обнаружив в нем потенциально охраняемый контент или персональные данные третьих лиц, принял решение совершить сделку, «закрыв» риски заверениями продавца о юридической «чистоте» датасетов. Либо если он вообще не сделает техническую экспертизу предобучающего датасета, имея такую возможность, но при этом в будущем будет пытаться компенсировать убытки, опираясь на заверения.

Поэтому в рамках сделки с ИИ-активами большую роль играют данные технической экспертизы и участие команды технических специалистов также на этапе подготовки документов по сделке и согласования защитных механизмов. Без этих компетенций юристам будет сложно правильно определить весь набор рас-

крытых сведений в отношении ИИ-модели и связанных с ней артефактов (весов, конфигураций, описания архитектуры и т. п.) для целей проработки механизмов транзакционной защиты покупателя. Для продавца такие сведения тоже крайне важны. Он обязан сообщить (раскрыть) покупателю наиболее важные из них вне зависимости от запроса заверений с его стороны. Это необходимо для соблюдения стандарта объективной добросовестности, требующего предоставить контрагенту по сделке всю значимую информацию, которая может повлиять на его решение совершить сделку.

В тех случаях, когда информация об ИИ-модели и других технологических аспектах будет объективно недоступна, в том числе в публичном поле, покупателю следует это фиксировать. Это обстоятельство «извиняет» его неосмотрительность и приравнивает его поведение при заключении сделки к добросовестному и разумному, несмотря на повышенные риски приобретаемого актива.

Раздел 3

Распределение ИИ-специфических рисков между сторонами сделки M&A

АВТОРЫ



Анастасия Нерчинская



Александр Панов
VERBA LEGAL



Роман Головацкий
DENUO

Краткие выводы

- Подходы к сопровождению сделок M&A с ИИ-компаниями, ключевым активом которых является ИИ-система, отличаются от «классических», применяемых в сделках с бизнесами, не использующими ИИ-технологии. Это обусловлено тем, что на традиционный ИТ-стек наслаивается ИИ-компонента, функционирование которой имеет специфику, требующую адаптации методологии работы с рисками.

- ИИ-технологии порождают ряд системных (архитектурных) рисков, которые не могут быть справедливо перераспределены между сторонами сделки стандартными договорными механизмами (например, с помощью обязательств о возмещении имущественных потерь) или внедоговорными инструментами (например, путем прямого уменьшения покупной цены). Основная причина этого в том, что «лучшим носителем» таких рисков является третье по отношению к сделке лицо[42] — разработчик модели, являющейся базовым ИИ-компонентом системы.

- Традиционный подход, при котором покупатель стремится перенести на продавца все выявленные исторические риски с помощью комбинации средств правовой защиты, не применим к ИИ-компаниям, использующим сторонние базовые модели. Продавец не может и не должен давать гарантии в отношении неподконтрольных ему аспектов ИИ-системы. Эти обстоятельства относятся к зоне предпринимательского риска покупателя и в соответствии со стандартом «лучших практик» принимаются им без дисконта к цене.

[42] За исключением крупнейших ИТ-экосистем, владеющих полной ИИ-вертикалью, включая собственные базовые модели.



Анатолий Земцов
DFCenter

- Основной критерий распределения ответственности в отношении поведения ИИ-системы — степень фактического контроля различных ее компонентов. Объем ответственности продавца (оператора ИИ-системы) должен соответствовать его возможностям по управлению соответствующим технологическим слоем: чем больше у него возможностей доступа к сторонним артефактам ИИ-технологии — весам, коду, архитектуре и датасетам модели, — тем шире зона управления рисками и ответственности оператора.

- Условно все риски функционирования ИИ-систем можно разделить на: (i) полностью подконтрольные продавцу (собственные дообучающие датасеты, RAG, оркестрация, системные промпты, прочие «надстройки» над моделью и т. п.); (ii) частично подконтрольные (точность ответов, галлюцинации, алгоритмическая предвзятость, безопасность на прикладном уровне); (iii) неподконтрольные (предобучающие датасеты модели, ее архитектура, алгоритмы обучения) — продавец не должен отвечать за эти риски.

- «Наследуемые» риски базовой модели практически не устранимы с помощью разумных или доступных оператору системы средств митигации — удаление датасета или его фрагментов не «очищает» уже обученные веса модели. Зачастую требуется полное переобучение модели «с нуля» на очищенном массиве данных (затраты сопоставимы с первоначальным обучением) либо применения экспериментальных методов Machine Unlearning (на сегодня — мало доступная технология).

- Инструментарий заверений имеет ряд серьезных ограничений, не позволяющих сторонам сделки эффективно распределить исторические риски бизнеса. Для этих целей эффективнее использовать механизмы возмещения имущественных потерь, а также отложенного обусловленного платежа. Особенно это относится к ситуациям, когда покупатель стремится закрыть специфические ИИ-риски, связанные, например, с дрейфом модели, интегрированной в продукт, безопасностью ее ответов или алгоритмическим смещением.

- При использовании механизма возмещения имущественных потерь для распределения ИИ-рисков, связанных с конкретными техническими параметрами, крайне важно сделать все необходимые измерения показателей на дату, близкую к дате подписания или закрытия сделки. Важно помнить, что покупателю придется доказывать не просто факт отклонения от метрик, установленных формулировкой триггера, но и их первопричину, а также то, что она относится к периоду до закрытия сделки. Для этого может потребоваться не просто фиксация метрик на дату закрытия сделки, но и данные динамического мониторинга, в том числе их ретроспективный анализ. О доступе к таким данным следует подумать до закрытия сделки.

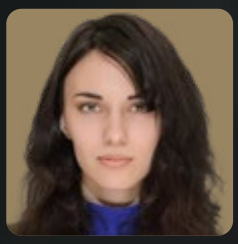
- Сложность доказывания причинно-следственной связи между согласованным сторонами основанием возмещения имущественных потерь и самими потерями заключается в том, что в ИИ-активах такие потери могут возникнуть по причинам (в том числе «сработавшим» одновременно): (i) наличия у ИИ-системы скрытых дефектов на уровне данных, кода или архитектуры, за которые отвечает продавец; (ii) изменившихся условий эксплуатации системы после закрытия сделки, например, смены источника входных данных или сегмента аудитории, за которые отвечает покупатель; (iii) решений вендора (разработчика модели), принятых в том числе до закрытия сделки; (iv) стечения случайных факторов, например, дрейфа, который может вызвать усиление алгоритмического смещения и наоборот.

Покупатели бизнесов, выявив при проведении due diligence исторические риски приобретаемого бизнеса, стремятся учесть их в цене с помощью различных инструментов. Стоимость высоких неустранимых рисков, если они не привели к срыву сделки, иногда напрямую вычитается из цены. В большинстве иных случаев стороны договариваются о перераспределении рисков с помощью договорных механизмов.

Почему в сделках с ИИ-активами этот подход не работает в полной мере?

Ответ кроется в природе рисков ИИ-активов и возможности их контроля участниками сделки. В проектах с традиционными активами продавец далеко не всегда готов отвечать за ряд дефектов бизнеса. Например, он может быть не полностью уверен в степени осмотрительности операционной команды при решении ею тех или иных вопросов, по которым покупатель просит гарантии. Покупатель также понимает, что «все идеально быть не может», поэтому идет на определенные уступки в ходе переговоров. Но в целом — большинство исторических дефектов актива — это проблема не покупателя, а продавца, поскольку он является их «наиболее эффективным носителем». Это означает, что он лучше, чем кто-либо другой, осведомлен о причинах таких рисков и может их урегулировать с большим успехом, чем покупатель или иное лицо.

В ИИ-бизнесах «лучший носитель» многих рисков находится за пределами договоренностей продавца и покупателя. Чаще всего — это разработчик базовой модели, который не имеет никакого отношения к частной сделке третьих лиц. К нему нельзя прийти и попросить принять на себя часть рисков, которые покупатель ИИ-компании, использующей ИИ-систему, выявил по итогам due diligence. Но и переносить многие из таких рисков полностью на продавца – далеко не всегда справедливо по той причине, что он их не контролирует, не может на них повлиять и сам принял их на свой предпринимательский риск. Поэтому традиционный подход к распределению рисков в сделке M&A с ИИ-активами требует существенной адаптации.



Анастасия Нерчинская

Основной проблемой распределения рисков, связанных с дефектами ИИ-систем, является сложность установления причинно-следственной связи при возникновении различных инцидентов в ее работе и вызванных ими неблагоприятных последствий. Далеко не всегда возможно достоверно определить, кто отвечает за причину сбоя в функционировании ИИ-системы, — ее оператор, управляющий жизненным циклом конечного продукта, или разработчик базовой модели.

Эта неопределенность не является временным техническим недостатком, который может быть устранен по мере развития технологии и адаптации подходов к анализу ИИ-рисков. Напротив, она имманентно свойственна архитектуре ИИ-технологии, поэтому определенные категории рисков принципиально не могут быть проверены, перераспределены или устранены усилиями сторон сделки. Работа ИИ-системы всегда будет связана с рядом существенных рисков. Поэтому на текущем этапе развития технологии они не могут быть полностью перенесены на продавца и должны быть приняты покупателем без существенного дисконта к стоимости компании.

Разработчик прикладного ИИ-решения в процессе его эксплуатации осуществляет лишь высокоуровневое управление ИИ-моделью, к внутреннему устройству которой у него нет доступа. Эта особенность требует изменения традиционных подходов к юридическому структурированию подобных сделок и, в первую очередь, использованию механизмов распределения рисков. Фокус смещается с попытки полного переноса на продавца ответственности за материальные исторические дефекты в сторону многоуровневого распределения рисков.

3.1 Подход к распределению рисков

В сделке M&A с ИИ-активами продавец далеко не всегда является «лучшим носителем» ряда исторических рисков. Стандарт «обычной деловой практики», обеспечивающий справедливый баланс интересов каждой стороны, предполагает, что продавец принципиально не может отвечать за риски, которые ему абсолютно не подконтрольны.

Чтобы распределить риски, связанные с ИИ, между сторонами сделки M&A, нужно понимать границы ответственности продавца и предпринимательского риска покупателя. Для соблюдения оптимального баланса интересов сторон важно уже на начальных этапах сделки определить области контроля и ответственности продавца (оператора ИИ-системы) и отграничить их от сфер, находящихся вне его доступа и влияния.

В бизнесе, основанном на применении ИИ-технологий, существует несколько категорий рисков. Это риски, за которые продавец:

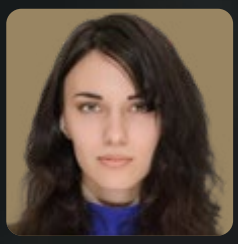
- **может отвечать полностью;**
- **не может (не должен) отвечать в принципе — их принимает покупатель;**
- **может отвечать, но лишь частично** и в строго ограниченных пределах, обусловленных техническими особенностями функционирования ИИ-системы.

Без понимания особенностей отдельных категорий рисков продавец ИИ-бизнеса может попасть в «ловушку» слишком широкой ответственности. В силу новизны технологии транзакционные команды, выступающие на стороне покупателя, все еще используют привычные им подходы и работают с ИИ-активами, как с «обычными». А именно — стремятся перенести на продавца **все** выявленные исторические риски путем использования различных договорных механизмов. Также M&A-эксперты пытаются работать с первопричинами ИИ-рисков, пытаясь сформулировать некий комплекс мероприятий, чаще всего технического характера, который позволил бы устранить или снизить соответствующие риски. Например, в рамках периода между подписанием и закрытием сделки, включив такие мероприятия в перечень отлагательных условий закрытия сделки.

Выбирая базовую модель для целей создания ИИ-системы, ее разработчик, как и любой последующий ее владелец, должны понимать, какая именно ИИ-технология лежит в основе прикладного решения, как и возможные риски. Последствия ложатся на сторону, которая согласилась использовать соответствующий актив в своем бизнесе.

Однако в работе с ИИ-активами **такие подходы требуют максимальной осторожности**. Это важно для продавца, чтобы он не оказался вынужден отвечать за множество потенциальных нарушений, которые может «создавать» ИИ-актив.

Но и для покупателя понимание такой «матрицы» рисков имеет существенное значение. Убедив продавца прогарантировать риски, за которые тот не отвечает и повлиять на них не может, — он будет рассчитывать на то, что эти средства защиты (в первую очередь, заверения) сработают в случае возникновении спора. От наличия таких гарантий может зависеть цена сделки. Однако не вполне ясно, как сработают в суде такие «широкие» гарантии, если они даны в отношении принципиально неустранимых рисков.



Анастасия Нерчинская

Даже если продавец примет на себя договорную ответственность в отношении ИИ-рисков, «наследуемых» от базовой модели, — покупатель впоследствии может столкнуться с большими сложностями процессуального характера, в том числе при формировании доказательственной базы. Чтобы подтвердить, что ИИ-инцидент, вызвавший неблагоприятные последствия, является прямым следствием нарушения заверений или обязательств продавца, потребуется доступ к технической «начинке» базовой модели, который вряд ли будет предоставлен.

К тому же продавец в некоторых случаях может выдвинуть довод о том, что покупатель, вступая в сделку, не мог не знать, что ИИ-технология, используемая в рамках приобретаемого бизнеса, заведомо сопряжена с повышенными и неустранимыми рисками, которые не контролирует продавец. Их материализация — зона предпринимательского риска покупателя.

Поэтому подходы к установлению оснований и пределов ответственности продавца ИИ-бизнеса должны оцениваться с точки зрения наличия у него принципиальной возможности отвечать за такие риски.

3.2 Разграничение зон ответственности

Степень контроля и уровень ответственности за риски, связанные с функционированием ИИ-системы, зависят от формата использования базовой модели в процессе ее интеграции с ИИ-системой. В частности, речь идет от **трех ключевых форматах**:

1. **Закрытая ИИ-модель** (closed-weight)

Продавец (оператор ИИ-системы) контролирует прикладной сервис, построенный «поверх» базовой ИИ-модели, но не саму базовую модель, ее веса, процесс ее обучения, архитектуру и внутренний технологический стек поставщика модели. **Его ответственность ограничена «надстройкой», абсолютное большинство рисков, связанных с моделью, находятся за пределами его контроля**.

2. **Закрытая ИИ-модель** (closed-weight)

Продавец (оператор ИИ-системы) имеет прямой доступ к весам (параметрам) модели и в ряде случаев к некоторым другим ее артефактам (например, файлам с кодом инференса и конфигурациями). Остальные элементы модели остаются закрытыми, включая предобучающие датасеты. Это позволяет ему контролировать уже не только сервис-надстройку над базовой моделью, но и **в определенной степени управлять самой моделью** в части ее развертывания, настройки, обработки входных данных. И, соответственно, **отвечать за эти процессы и напрямую связанные с ними риски базовой модели**.

3. **ИИ-модель с открытым исходным кодом и архитектурой** (open source)

Продавец (оператор системы) использует модель, в отношении которой доступен полный стек: веса, код, архитектура, обучающие датасеты и иные компоненты, позволяющие изучать, дообучать, модифицировать, воспроизводить и масштабировать модель. Здесь **зона контроля продавца максимальна, и, соответственно, таков же объем потенциальной ответственности по сделке**.

Ключевой принцип распределения ответственности оператора ИИ-системы таков — **объем ответственности должен соответствовать степени фактического контроля над соответствующим слоем ИИ-системы**.

В таблице ниже в наиболее общем виде приведены индикативные подходы к разграничению ответственности оператора ИИ-системы, основанной на сторонней базовой модели.

Матрица ответственности оператора ИИ-системы по критерию контроля над ее технологическими слоями

УРОВЕНЬ ИИ-СИСТЕМЫ	ЗАКРЫТАЯ МОДЕЛЬ (API)	МОДЕЛЬ С ОТКРЫТЫМИ ВЕСАМИ	МОДЕЛЬ С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ
1. Модель (веса)	НЕ ОТВЕЧАЕТ — за происхождение модели (весов); — корректность и «чистоту» предобучения и дообучения модели; — отсутствие скрытых дефектов, ошибок, хранение, развертывание, модификацию; — «тонкую настройку» и другие форматы дообучения, поведение модели ОТВЕЧАЕТ — за выбор модели и ее разработчика; — соблюдение лицензионных требований; поставщика базовой модели, включая экспортные, санкционные и территориальные ограничения, а также технические ограничения самой модели	НЕ ОТВЕЧАЕТ — за происхождение модели (весов); — корректность и «чистоту» предобучения модели; — отсутствие скрытых дефектов и ошибок, возникших в результате предобучения модели ОТВЕЧАЕТ — за выбор модели и ее разработчика; — соблюдение лицензионных условий; — хранение, развертывание, модификацию; — «тонкую настройку» и другие форматы дообучения модели разработчиком системы и связанные с ним ошибки и дефекты поведения модели	НЕ ОТВЕЧАЕТ — за происхождение модели (весов); — корректность и «чистоту» предобучения модели; — отсутствие скрытых дефектов и ошибок, возникших в результате предобучения модели ОТВЕЧАЕТ — так же, как и в сценарии использования модели с открытыми весами. Но поскольку оператору системы изначально доступно больше артефактов модели, это расширяет возможности white-box проверки модели, особенно если открыты предобучающие датасеты, что повышает стандарт осмотрительности как продавца, так и покупателя
2. Модель (архитектура, исходный код, инференс)	НЕ ОТВЕЧАЕТ — за архитектуру и исходный код базовой модели	НЕ ОТВЕЧАЕТ — за исходный код и архитектуру ОТВЕЧАЕТ ЧАСТИЧНО — за совместимость; — интеграцию; — отдельные технические аспекты, но не за изначальный дизайн архитектуры, если он унаследован от третьего лица и не раскрыт полностью	ОТВЕЧАЕТ В ЗНАЧИТЕЛЬНОЙ СТЕПЕНИ — за код и архитектуру, особенно если они доступны и продавец их модифицировал или использовал как основу собственного сервиса

УРОВЕНЬ ИИ-СИСТЕМЫ	ЗАКРЫТАЯ МОДЕЛЬ (API)	МОДЕЛЬ С ОТКРЫТЫМИ ВЕСАМИ	МОДЕЛЬ С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ
3. Данные (обучающие датасеты)	НЕ ОТВЕЧАЕТ — за предобучающие датасеты, не контролирует их и не имеет доступа ОТВЕЧАЕТ — за собственные датасеты, если они использовались для адаптации модели через инструменты API	НЕ ОТВЕЧАЕТ — аналогично сценарию использования закрытой модели ОТВЕЧАЕТ — за собственные обучающие датасеты и прочие наборы данных, включая их состав, качество и юридическую «чистоту», если они использовались для адаптации модели. **Исключение**: невозможность контроля отдельных наборов данных (например, в веб-модели динамического RAG)	НЕ ОТВЕЧАЕТ — за предобучающие датасеты, если к ним нет доступа (не все open source модели раскрывают их) МОЖЕТ ОТВЕЧАТЬ — за хранение и использование предобучающего датасета, если он доступен, поскольку в этом случае имеется возможность white-box тестирования такого датасета ОТВЕЧАЕТ — за собственные датасеты, если они использовались для адаптации модели
4. Данные (результаты «тонкой настройки»)	ОТВЕЧАЕТ ПОЛНОСТЬЮ — за собственный результат «тонкой настройки»	ОТВЕЧАЕТ ПОЛНОСТЬЮ — поскольку контролирует процесс дообучения	ОТВЕЧАЕТ — так же, как в сценарии использования модели с открытыми весами
5. Данные (адаптация без дообучения, включая RAG)	ОТВЕЧАЕТ ПОЛНОСТЬЮ — если данные, используемые для адаптации модели, в том числе в «базе знаний» RAG, прямо или косвенно контролируются продавцом. В этом случае продавец отвечает за качество и точность понимания контекста запроса, точность индексации, актуальность и релевантность выдаваемых дополнительных данных, права на такие данные НЕ ОТВЕЧАЕТ — за данные, которые не контролируются и не могут контролироваться продавцом	ОТВЕЧАЕТ — так же, как в сценарии использования закрытой модели	ОТВЕЧАЕТ — так же, как в сценарии использования закрытой модели

УРОВЕНЬ ИИ-СИСТЕМЫ	ЗАКРЫТАЯ МОДЕЛЬ (API)	МОДЕЛЬ С ОТКРЫТЫМИ ВЕСАМИ	МОДЕЛЬ С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ
6. **Оркестрация и системные промпты**	ОТВЕЧАЕТ ПОЛНОСТЬЮ — если именно продавец определяет системные промпты, роутинг, вызов инструментов	ОТВЕЧАЕТ ПОЛНОСТЬЮ	ОТВЕЧАЕТ ПОЛНОСТЬЮ
7. **Традиционное ПО в рамках ИИ-системы**: интерфейс сервиса, бизнес-логика, инструментальное ПО (оркестраторы, СУБД и т. п.)	ОТВЕЧАЕТ ПОЛНОСТЬЮ	ОТВЕЧАЕТ ПОЛНОСТЬЮ	ОТВЕЧАЕТ ПОЛНОСТЬЮ
8. **Безопасность ответов модели**	НЕ ОТВЕЧАЕТ — за ограничения и политики безопасности, реализованные на уровне базовой модели, если не может ими управлять ОТВЕЧАЕТ — в существенной степени на уровне системы за процессы организации, фильтрации и модерации контента; установление пользовательских ограничений; создание и соблюдение комплаенса протоколов, протоколов безопасности	ОТВЕЧАЕТ ПОЛНОСТЬЮ — на уровне системы, включая максимально быстрое выявление нарушений и актуализацию соответствующих политик и процедур	ОТВЕЧАЕТ — так же, как в сценарии использования модели с открытыми весами
9. **ИБ**	ОТВЕЧАЕТ — за информационную безопасность собственного приложения (ИИ-системы), ключей API; — соблюдение установленных процедур взаимодействия с разработчиком базовой модели	ОТВЕЧАЕТ ПОЛНОСТЬЮ — за исключением кода базовой модели, относящегося к архитектуре модели и связанных с ней компонентов	ОТВЕЧАЕТ ПОЛНОСТЬЮ

УРОВЕНЬ ИИ-СИСТЕМЫ	ЗАКРЫТАЯ МОДЕЛЬ (API)	МОДЕЛЬ С ОТКРЫТЫМИ ВЕСАМИ	МОДЕЛЬ С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ
10. **Технические характеристики системы** (скорость работы, предел нагрузки / пропускная способность, отказоустойчивость и т. д.)	ОТВЕЧАЕТ ЧАСТИЧНО — в пределах ИИ-системы и SLA перед конечными пользователями НЕ ОТВЕЧАЕТ — за технические характеристики серверной инфраструктуры и технологического стека базовой модели	ОТВЕЧАЕТ — полностью в части ИИ-системы, включая перенастроенные / модифицированные параметры локализованной базовой модели	ОТВЕЧАЕТ ПОЛНОСТЬЮ
11. **Качество, точность, отсутствие галлюцинаций и предвзятости модели**	НЕ ОТВЕЧАЕТ — за качество, точность, отсутствие галлюцинаций и предвзятости базовой модели в части, в которой продавец (разработчик ИИ-системы) на них не влияет и не может влиять ОТВЕЧАЕТ ЧАСТИЧНО — за поддержание указанных характеристик модели в пределах, в которых сам может влиять на них, а также за меры по предупреждению, мониторингу и своевременному выявлению нарушений таких характеристик	ОТВЕЧАЕТ ЧАСТИЧНО — в пределах собственного влияния на изменение таких характеристик модели, а также за меры по предупреждению, мониторингу и своевременному выявлению нарушений таких характеристик	ОТВЕЧАЕТ — так же, как в сценарии использования модели с открытыми весами

Логику использования транзакционных механизмов распределения рисков в сделке M&A с ИИ-компанией целесообразно выстраивать, исходя из индикативного подхода, отраженного в таблице. Это — ориентир, показывающий базовые принципы распределения ответственности в зависимости от степени контроля и глубины управления этапами жизненного цикла ИИ-системы. В реальности границы ответственности могут быть еще более размытыми и неопределенными, особенно в части рисков, за которые оператор системы «делит» ответственность за работу модели.

3.3 Категории рисков ИИ-системы

3.3.1 Неустранимые («наследуемые») риски

Если следовать рассмотренной выше логике, риски, которые могут считаться **принципиально неустранимыми**, — это преимущественно те риски, за которые, как указано в таблице, разработчик ИИ-системы (продавец) полностью не отвечает. Они сконцентрированы в слое базовой модели и связаны с ее предобучением, юридической и технической «чистотой» данных, используемых разработчиком модели для целей ее создания и эксплуатации. У продавца (оператора системы) отсутствует доступ к технологической «начинке» и соответствующей информации и возможности управления и контроля в отношении этих вопросов.

Стандарт «лучших практик» не предполагает гарантий продавца в отношении таких рисков при симметричности переговорных позиций сторон.

Однако продавец может добровольно согласиться предоставить гарантии в отношении аспектов сторонней базовой модели (например, юридической «чистоты» предобучающего датасета) или иным образом принять за них ответственность перед покупателем. Такой сценарий будет явно выходить за рамки нормального переговорного стандарта, отражая более слабую позицию продавца.

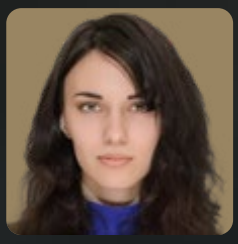


Илья Булгаков

советник

DÉNUO

Необходимо понимать, что сделки с ИИ-активами относительно новые на рынке, а заверения — это институт перераспределения экономических рисков сторон. Подходы к тому, какая сторона сделки должна нести соответствующий экономический риск, только формируются, поэтому многое в конечном счете зависит от переговорной силы сторон и риск-аппетита покупателя. Иногда именно это является причиной того, что пока что в финальной версии документации заверения относительно самих ИИ-моделей не включаются или включаются в усеченном виде.



Анастасия Нерчинская

Даже если продавец ИИ-компании сам получил какие-либо гарантии от разработчика модели (что представляется исключительно редким случаем) или поставщика иных ресурсов, например датасетов, — такие гарантии не «очищают» права на соответствующие активы и не создают субъективной добросовестности на стороне продавца (оператора ИИ-системы) и его контрагента по сделке M&A — покупателя. Иными словами, если при формировании датасета были использованы охраняемые объекты третьих лиц без их согласия, то никакие гарантии не снимут ответственность с указанных выше лиц, они все равно будут отвечать перед владельцем контента или регулятором или за допущенные нарушения.



Роман Головацкий

партнер

DÉNUO

@DENUOLAW →

Несмотря на отсутствие на текущий момент устоявшейся практики сопровождения сделок с ИИ-решениями, очевидно, что традиционные подходы не могут быть применены здесь в полном объеме. В отличие от классического программного обеспечения, уровень контроля разработчика ИИ-системы над юридической и функциональной «чистотой» своего продукта существенно ниже.

Специфика большинства ИИ-бизнесов такова, что их технологический стек базируется на сторонних базовых моделях, которые находятся под полным контролем третьих лиц. Это влечет за собой появление рисков, которые нетипичны для классических сделок, например, таких как одностороннее изменение условий API-доступа к модели, изменение логики ответов модели («дрейф модели»), неправомерный состав исходных обучающих данных.

Безусловно, степень автономности разработчика ИИ-системы напрямую зависит от формата дистрибуции базовой модели. В случае закрытых моделей влияние вендора является практически абсолютным, а юридические гарантии ограничены условиями лицензии (чаще всего это формат «as is»). Использование же открытых (open source) моделей предоставляет большую гибкость, однако и здесь контроль остается ограниченным из-за зависимости от предобучающих датасетов и архитектурных решений, заложенных разработчиком модели. Таким образом, при структурировании сделок с ИИ-решениями формулирование заверений об обстоятельствах требует учета этих технологических зависимостей и соответствующего распределения рисков между продавцом и покупателем.

3.3.2 Риски, подконтрольные продавцу

Аспекты ИИ-бизнеса, в отношении которых покупатель может при наличии рисков обоснованно запрашивать гарантии в полном объеме, относятся ко всему прикладному слою «поверх» модели, включая данные, которые использовались для дообучения модели или иных методов ее адаптации. Они полностью или преимущественно подконтрольны разработчику ИИ-системы. Здесь допустимо и разумно использовать классические транзакционные подходы. Покупатель, понимая, что эти процессы находятся в зоне влияния продавца и его операционной команды, будет запрашивать традиционно широкий объем средств правовой защиты от рисков. Продавец же будет стремиться ограничить свою ответственность, используя стандартные квалификаторы знания, материальности и другие оговорки.

3.3.3 Риски, частично контролируемые продавцом

Это — самая сложная категория рисков, поскольку продавец может отвечать за риск, но лишь частично. Такой риск условно «делится» с разработчиком модели. Это касается преимущественно технических аспектов функционирования ИИ-системы, в том числе точности и безопасности ответов модели, на которые уже могут влиять не только действия разработчика модели, но и оператора системы (продавца).

Здесь кроется множество нюансов, так как объективно установить такую «точку отсчета» для компании очень сложно. Для этого ей как оператору ИИ-системы необходимо на регулярной основе проводить измерение и мониторинг ключевых параметров поведения модели, в первую очередь влияющих на характеристики дрейфа, алгоритмической предвзятости и безопасности на прикладном уровне. Чтобы ИИ-компания и ее продавец могли «защитить» себя от излишней ответственности, целесообразно своевременно внедрить соответствующую систему ИИ-комплаенса.

Для продавца будет важно опираться на такие параметры и при согласовании текста заверений и других защитных положений, предложенных покупателем. Так, стороны могут согласовать обусловленный отложенный платеж с привязкой части цены к факту нереализации некого технического триггера (например, к отсутствию случаев падения точности ответов модели ниже согласованных в договоре параметров в течение года после закрытия сделки). В такой ситуации стороны столкнутся с той же необходимостью — иметь ориентир в виде метрик и объективных данных, чтобы обосновать наступление триггера. Если продавец не внедрил процедуры журналирования, логирования, мониторинга показателей функционирования ИИ-системы, — средство защиты, связанное с соответствующим обстоятельством, которое не удалось верифицировать, не будет эффективно реализовано, и сделка может быть совершена на менее выгодных ценовых условиях для продавца.



Анатолий Земцов

управляющий партнер

dfcenter

Продавец может давать обоснованные гарантии только в пределах своей фактической зоны контроля. Он не может подтверждать состав, источники и правовой статус «чужих» обучающих данных, если сам не участвовал в их формировании и не имеет доступа к соответствующей документации.

Для корректного разграничения ответственности в договоре желательно зафиксировать:

- Перечень данных, созданных или обработанных продавцом (с указанием их объема, назначения и статуса).
- Описание базовой модели как внешнего компонента, предоставляемого по лицензии.
- Границы контроля продавца (fine-tuning, конфигурация, интеграция, тестирование).
- Отказ от гарантий в части исходных обучающих данных базовой модели, если такие гарантии не предоставлены ее разработчиком (правообладателем), и указание, что соблюдение требований к обучающим данным базовой модели относится к зоне ответственности правообладателя модели.

Например, разделение зон ответственности может быть описано через архитектурную декомпозицию решения: «базовая модель», «дополнительное обучение / адаптация», «собственные датасеты продавца», «прикладная логика и интеграция». В договоре это оформляется как разграничение гарантий по компонентам системы и указание на отсутствие контроля над исходным обучающим корпусом модели.

3.4 Мероприятия по устранению рисков

В связи с фактически неустранимым характером некоторых рисков, свойственных ИИ-системам, возникает вопрос — а может ли участник сделки самостоятельно предпринять какие-либо меры по смягчению таких рисков?

Существуют заблуждения о пределах возможностей по митигации ИИ-специфических рисков путем «исправления» дефектов, выявленных в рамках due diligence ИИ-систем. Например, о том, что если проверка обнаружит риски, связанные с воспроизведением ИИ-системой объектов авторского права или персональных данных, принадлежащих третьим лицам, то покупатель сможет потребовать от ИИ-компании устранить эти риски с помощью реализации мероприятий технического характера. Некоторые эксперты даже предлагают включать требование о выполнении компанией таких мероприятий напрямую в транзакционную документацию в качестве отлагательных условий.

Здесь следует понимать, что в отношении мероприятий по устранению ИИ-рисков **действуют те же самые принципы** определения пределов влияния разработчика ИИ-системы на поведение ИИ-компоненты и возможностей собственного вмешательства. Что-либо «исправить» путем реализации конкретных мероприятий **можно только в отношении тех аспектов, которые контролирует непосредственно разработчик ИИ-системы**. Это относится к слою дообучающих данных или иным методам адаптации модели, не связанным с дообучением модели, например, RAG, а также иным «надстройкам» поверх базовой модели, сделанным непосредственно оператором системы либо под его контролем.

Если же речь идет об устранении рисков на уровне слоя базовой модели — предобучающих датасетов или ее алгоритмов принятия решений, — в этом случае у оператора системы (и продавца бизнеса) нет реальных инструментов и возможностей что-либо исправить по существу. Вряд ли продавец сможет потребовать от разработчика модели удалить модель, переобучить ее или применить иные технологии, которые обеспечили бы «забвение» моделью конкретных обнаруженных данных, которые стали причиной риска.

> **Что-либо «исправить» путем реализации конкретных мероприятий можно только в отношении тех рисков, которые контролирует разработчик ИИ-системы.**



Анатолий Земцов

управляющий партнер

dfcenter

Существует точка зрения, что проблема юридически «грязного» датасета (IP-нарушения, персональные данные), на котором обучалась модель, может быть разрешена путем удаления этого датасета либо «перенастройкой» модели. В этом вопросе не все так однозначно.

Если компания обучала (дообучила) модель на «грязном» датасете, то эти «токсичные» данные уже вшиты в миллионы и миллиарды параметров нейросети. Удаление датасета устранит риск дальнейшего распространения и, возможно, удовлетворит требование регулятора в части удаления данных. Но на модель это уже не повлияет, она уже «знает» эти данные в своих весах.

Чтобы максимально надежно снять риск, нужно провести полное переобучение, то есть обучить модель заново на гарантированно «чистом» датасете. Для этого, соответственно, нужна необученная версия модели и чистый датасет. Стоимость и трудозатраты на такую процедуру будут сопоставимы с самим первоначальным обучением.

Метод «забывания» (Machine Unlearning) потенциально тоже может решить эту проблему. Но с нюансами. Во-первых, это технология скорее исследовательского уровня, которая работает в определенных условиях и не дает стопроцентно гарантированного результата. Во-вторых, принципиально важно понимать, что целью забывания является не превращение модели в «чистый лист», а нечто более сложное: избирательное удаление влияния конкретных, проблемных данных из весов уже обученной модели, при котором все остальные, полезные знания, полученные из корректной части датасета, сохраняются. Процедура, по сути, эквивалентна точечному хирургическому вмешательству в веса, позволяющему избежать дорогостоящего и длительного полного переобучения. Только если эта операция не удалась и модель была необратимо повреждена, придется прибегнуть к ее полному переобучению с нуля на чистом датасете.

Если проблема у компании-продавца возникла на уровне «загрязненных» векторов (без необходимости изменения весов) — ситуация, с технической точки зрения, проще. Грязные данные можно удалить из базы знаний. Конкретный чанк. При хорошем исходе после такой операции модель «забудет» удаленное и ничего не выдаст при следующем запросе, так как ей нечего будет выдавать из базы знаний. Однако эффективность метода может отличаться в разных условиях.

Самый же привлекательный вариант на сегодняшний день — это семейство методов на базе подхода SISA (Sharding, Incremental training, Slicing, and Aggregation). Он сводится к тому, что еще на этапе проектирования модели она создается как ансамбль минимоделей. И если в работе или в датасете, относящимся к какой-то из этих минимоделей, впоследствии обнаружится существенный изъян — переобучать необходимо только один маленький «кусочек», а не всю большую модель. Однако оговорюсь, для применения этой методики такая возможность должна быть заложена в архитектуру модели еще на этапе ее разработки и создания.

3.5 Заверения об ИИ-активах

В рамках исследования мы попросили экспертов рассказать о том, какой ТОП-3 ИИ-специфических заверений в отношении бизнеса на основе ИИ-системы они бы запросили, выступая на стороне покупателя такой ИИ-компании.



Асият Культербаева

советник

VERBA LEGAL

Прежде чем прописывать заверения для приобретения ИИ-бизнеса, необходимо дать исчерпывающие юридически точные определения всем ключевым активам: «ИИ-Технологиям» (включая модели, алгоритмы, архитектуры), «ИИ-Входам» (обучающие данные) и «ИИ-Выходам» (генерируемый контент, прогнозы). Эта терминологическая основа исключает двусмысленность и формирует каркас для специфичных заверений.

Три наиболее важные категории заверений, на которых я бы сфокусировалась как покупатель:

1. Заверения в отношении происхождения и прав на данные: продавец должен предоставить заверения о том, что он обладает всеми необходимыми правами и лицензиями на все данные, использованные для обучения моделей, включая явные согласия субъектов ПДн и соблюдение условий открытых лицензий. Критично также заверение в адекватности и репрезентативности этих данных для заявленных кейсов, чтобы избежать риска некорректной работы модели в целевой среде (например, чат-бот, обученный на личной переписке, не подходит для клиентского сервиса).
2. Заверения в отношении легальности выходных данных и отсутствия скрытых рисков: необходимо заверение, что компания имеет неоспоримое право на коммерциализацию выходных данных (outputs) своих ИИ-систем и что эти outputs не нарушают прав третьих лиц. Особое внимание — использованию генеративного ИИ (GenAI): продавец должен гарантировать, что такое использование не ставит под угрозу действительность или защиту интеллектуальной собственности компании (например, патентоспособности изобретений или авторских прав).
3. Заверения в отношении управляемости, безопасности и соответствия: это комплексная категория, включающая:
    - Техническую воспроизводимость и возможность переобучения моделей без непредвиденных ограничений.

- Внедрение разумных мер кибербезопасности для защиты моделей от кибератак, особенно для API-доступных систем.
- Соблюдение этических принципов и регуляторных требований.

Дополнительно незаменимы заверения в отношении полноты раскрытия всех ИИ-активов и сценариев их использования, так как риски для разных индустрий кардинально различаются.



Софья Смирнова

советник M&A
и корпоративной практики

O_2 консалтинг

Сделки в отношении ИИ-бизнесов представляют собой относительно новый класс сделок, для которого классический инструментарий заверений требует адаптации. Особенно это касается приобретения бизнесов, построенных на интеграции со сторонней ИИ-моделью. Архитектура рисков такого бизнеса принципиально отлична от классического IT-актива: ключевой ресурс (модель) не принадлежит и никогда не будет принадлежать приобретаемой компании, а результат использования ресурса подлинно не контролируем ни для продавца, ни для покупателя.

В этой связи три ключевых приоритета покупателя должны, по нашему мнению, выглядеть так (и по сути описывать ИИ-продукт как актив).

Во-первых, детальное договорное заверение об отношениях приобретаемой компании с провайдером базовой модели. Содержательно оно охватывает несколько уровней:

- Действительность и надлежащее оформление договора непосредственно на таргет.
- Соответствие фактических сценариев использования условиям сервиса, включая характерные для типовых соглашений зарубежных провайдеров ограничения относительно reverse engineering, обучения конкурирующих систем и географии использования.

- Отсутствие на момент закрытия оснований, которые впоследствии могли бы быть использованы провайдером для одностороннего прекращения отношений.
- Наконец, степень технологической подготовленности приобретаемого бизнеса к возможной миграции на альтернативную модель.

В российском контексте к этому неизбежно добавляется санкционный слой: значительная часть зарубежных API формально не допускает использования российскими юридическими лицами, и распространившаяся практика структурирования доступа через дружественные юрисдикции, не будучи раскрытой продавцом, формирует для покупателя отложенный риск утраты доступа уже после закрытия сделки.

Второй блок заверений касается законности данных и принадлежности интеллектуальных прав. Соответствующие риски, как правило, не материализуются непосредственно после закрытия — типичный сценарий предполагает их проявление спустя один–три года в связи с проверкой регулятора, претензией правообладателя или жалобой субъекта персональных данных. Заверения целесообразно распространить на законность всех источников данных, использованных для обучения, «тонкой настройки», RLHF[43] и RAG; на наличие согласий по 152-ФЗ, охватывающих именно цели обучения модели, а не неопределенные маркетинговые цели; на соблюдение требования о локализации; на чистоту обучающих датасетов от объектов авторского права третьих лиц, особенно с учетом того, что перечень допустимых случаев свободного использования произведений носит закрытый (исчерпывающий) характер; на надлежащее оформление прав на собственные РИД, в том числе в режиме ноу-хау или коммерческой тайны.

[43] Reinforcement Learning from Human Feedback — обучение с подкреплением на основе человеческих предпочтений.

Наконец, соответствие ИИ-продукта применимому законодательству. В классическом M&A без индустриальной «заточки» этот блок иногда формулируется как «общее соответствие законодательству» и не выделяется отдельно. Для ИИ-продукта такой подход недостаточен по двум причинам:

- Текущий статус приобретаемого бизнеса в регуляторной системе (участвует ли он в ЭПР[44], какие у него есть преимущества или, наоборот, обязательства) сам по себе является активом, требующим проверки (и, соответственно, заверений).
- Отраслевая специфика ИИ-применения может повлечь невозможность монетизации ключевого продукта: медицинский ИИ, финансовый ИИ, ИИ в обработке биометрии, ИИ в КИИ и даже юридический ИИ либо стали, либо могут стать предметом специального регулирования, и это критичный элемент статуса актива.

Отдельно очень важно отметить следующее: необходимо (а) придать данным заверениям статус «существенных», (б) разграничить заверения по стандарту знания: продавец отвечает за объективную достоверность фактов, находящихся в его контроле (титул, состояние договоров, корпоративная структура), и отвечает только за свою добросовестную осведомленность применительно к фактам, объективно не поддающимся полной проверке (поведение модели, потенциальные претензии третьих лиц, скрытые дефекты данных).

[44] Экспериментальный правовой режим.



Елена Полевая

старший юрист

KKMP LEGAL

Если ИИ имеет существенное значение для бизнеса приобретаемой компании мы, как покупатель, запросим следующие основные заверения:

1. **Заверения в отношении прав и законности использования ИИ-активов:**
   - Подтверждение титула на ИИ-активы или правомерности их использования.
   - Подтверждение законности получения и использования обучающих данных.
   - Подтверждение наличия исключительных прав на результаты генераций ИИ-модели.
2. **Заверения о корректной работе и качестве ИИ-активов:**
   - Функционирование ИИ-активов в соответствии с заявленными характеристиками.
   - Отсутствие в ИИ-инструментах существенных ошибок, дефектов или сбоев в работе.
   - Отсутствие скрытых зависимостей или ограничений со стороны третьих лиц.
3. **Заверения о соблюдении регуляторных норм:**
   - Соблюдение требований о конфиденциальности, безопасности и обработке данных.
   - Соблюдение применимых регуляторных норм к разработке и использованию ИИ.

Состав заверений зависит от роли продавца (разработчик модели, оператор системы, владелец сервиса, пользователь) и типа ИИ-актива. На практике многие сделки касаются прикладных ИИ-сервисов, основанных на сторонних моделях. В таких случаях владелец сервиса ограничивает заверения своей зоной контроля и, как правило, не может отвечать за разработчика модели, включая правомерность создания модели и обучающих данных. Если продавец совмещает несколько ролей, заверения целесообразно структурировать по технологическим слоям, чтобы обеспечить защиту для каждого ИИ-актива. В отношении генеративного ИИ, учитывая повышенные риски, заверения должны быть максимально детализированы.



Кристина Мкртчян

советник практики интеллектуальной собственности

ЭБР
Юридическая Компания

В ситуации, когда таргетом стала ИИ-компания с активом в виде ИИ-системы на основе сторонней базовой модели, следует включить в состав заверений положения о том, что:

- Выходные данные системы соответствуют заявленным характеристикам.
- Нет известных продавцу случаев существенных галлюцинаций (повлекших ущерб третьим лицам) или вредоносных выходных данных.
- Метрики качества, раскрытые покупателю, получены на репрезентативных тестовых выборках и не были намеренно улучшены.

Это важно, потому что, в отличие от традиционного ПО, «поведение» ИИ-продукта вероятностно и не покрывается исчерпывающе тестами. Продавец, который знает о «плохом поведении» ИИ-продукта (системных сбоях), например, в медицинском или юридическом контексте, может скрыть их. То есть по итогу показать cherry-picked бенчмарки, а на деле после закрытия сделки покупатель получает ряд негативных последствий, от репутационных издержек до несправедливой оценки таргета.

3.5.1 Аспекты на стороне продавца

При формулировании заверений продавцу ИИ-компании следует быть очень внимательным. К примеру, следует избегать фраз о том, что «компания соблюдает или не нарушает применимое законодательство, включая регулирующее ИИ и персональные данные». Даже если продавец будет использовать какие-либо квалификаторы, например о «существенной степени», — такое заверение применительно к ИИ-сфере все равно будет крайне широким, подразумевающим, что компания использует юридически «чистую» ИИ-технологию, что практически невозможно проверить и верифицировать в силу архитектурных особенностей ИИ.

Покупатели обоснованно запрашивают заверения о том, что ИИ-компания внедрила и соблюдает все необходимые политики и процедуры, направленные на обеспечение: (i) непредвзятых, точных и безопасных результатов (генераций); (ii) недопущение причинения вреда третьим лицам, а также (iii) достаточной степени человеческого контроля при использовании ИИ-технологий. В некоторых случаях покупатели просят указать в транзакционной документации конкретные метрики и пороговые значения, характеризующие поведение ИИ-модели. Прежде чем продавец согласится предоставить такие заверения, ему следует убедиться в том, что он действительно внедрил соответствующую систему мониторинга показателей, отслеживает и фиксирует их динамику, такие процедуры носят систематический характер и имеют надлежащее документальное оформление.

Максимально осторожно следует относится к заверениям о том, что компания владеет всей или существенной информацией, которая может объяснить (обосновать) решения, принятые с помощью использования ИИ-технологий (свойство т. н. «прозрачности» или «объяснимости»), а также, что компания хранит такую информацию в человекочитаемой или иной требуемой форме и может в любой момент предоставить ее по запросу. За исключением случаев, когда компания является разработчиком ИИ-модели, она с очень высокой степенью вероятности не располагает такой информацией. Более того, даже разработчик модели не всегда может обосновать те или иные ответы модели (феномен «черного ящика») с помощью доступного ему инструментария и информации.

> **Даже если оператор ИИ-системы получил какие-либо гарантии от стороннего разработчика базовой модели или поставщика датасета, — такие гарантии не «очищают» его (как и любого последующего приобретателя такого бизнеса) персональные риски в отношении этих активов.**

Также продавцу не следует соглашаться на предоставление заверения о том, что компания соблюдала (полностью или в существенной степени) все или конкретные отраслевые ИИ-стандарты, если это не соответствует действительности. При этом вполне разумно будет предоставить такую гарантию в отношении конкретно применимого стандарта или отдельных вопросов, подпадающих под его регулирование, если компания действительно использовала такую практику.

К гарантиям, которые затрагивают **обучающие датасеты или данные, следует относиться особенно внимательно**, так как именно они сопряжены **с максимальными рисками «излишней ответственности» для продавца**. Каждую такую гарантию, предложенную покупателем, следует оценивать на предмет того, к каким данным она относится. Если она касается обучающих данных, которые не контролирует продавец (не участвовал при формировании датасета или не приобретал его для целей

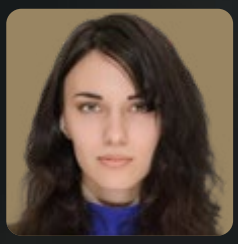
адаптации модели), желательно отказаться от предоставления такой гарантии. Продавец не может гарантировать «чистоту» таких данных.

Если из текста или контекста гарантии не исключить данные, на которых обучалась модель вне контроля продавца (а это может быть не только изначальный предобучающий датасет), то продавец автоматически примет на себя ответственность и за полностью не подконтрольные ему вопросы.

Также продавец ИИ-компании не может гарантировать покупателю получение всех согласий субъектов персональных данных (равно как и наличие всех иных правовых оснований для их обработки), даже в отношении датасетов, которые формировал сам. Такое заверение требует серьезного объема уточнений в рамках процедуры раскрытия информации. Получить все согласия гипотетически может только компания, которая сама формирует датасеты, то есть использует собственные массивы данных. Однако для целей дообучения модели такая ситуация является скорее исключением, поскольку обычно компании используют большие объемы публичных данных, не ограничиваясь рамками собственных датасетов.

Также существенной настороженности требуют заверения о юридической «чистоте» ответов ИИ-системы и, в особенности, — об отсутствии скрытых дефектов ИИ-системы.

Если покупатель запрашивает гарантии в отношении конкретных метрик поведения модели, интегрированной в ИИ-систему, для покупателя важно **избегать заверений об «основаниях» возникновения отклонений соответствующих параметров**, например о том, что на дату сделки продавцу не известно о наличии каких-либо причин для возникновения у продукта значимых галлюцинаций, которые могли бы привести к причинению вреда. Все замеры таких метрик целесообразно произвести максимально близко к соответствующей дате предоставления гарантии. При этом в документации следует оговориться, что соответствующая гарантия предоставляется исключительно на дату совершения или закрытия сделки и не распространяется на прошлое и будущее время, особенно если речь идет о динамических параметрах с нелинейной динамикой. Если покупатель запросит данные об изменении таких показателей во времени (например, средний «шаг» дрейфа модели за определенный период), такие заверения можно предоставить с оговоркой, что параметры были измерены на определенную дату, на конкретном датасете, инфраструктуре и обучающей среде, и продавец не несет никакой ответственности за их экстраполяцию покупателем на любые другие обстоятельства и условия.



Анастасия Нерчинская

Сторонам сделки, и особенно продавцу, следует быть очень внимательными при формулировании заверений в отношении ИИ-компании. Это тот случай, когда любое лишнее слово может расширить ответственность продавца. На сегодняшний день еще не сформировался подход к работе с заверениями в отношении ИИ-активов. Поэтому в сделках все еще встречаются стандартные формулировки заверений, логика которых предполагает, что продавец прямо или косвенно контролирует соответствующие аспекты. Однако в сделках с ИИ-компаниями это может привести к тому, что даже на первый взгляд безобидные заверения могут стать поводом для необоснованно широкой ответственности продавца, если она распространится и на уровень базовой модели.

В транзакционной документации и в процессе коммуникаций по сделке очень важно на уровне терминов четко разграничивать ситуации предобучения и дообучения ИИ-модели, осуществляемые третьей стороной, и дообучения модели при ее адаптации, которое производит непосредственно оператор системы. Зачастую эти категории данных смешиваются или описываются сложным для восприятия образом, в том числе для этого могут использоваться несколько терминов, что крайне затрудняет чтение и понимание документации.

Если продавец ИИ-бизнеса соглашается предоставить покупателю какие-либо ИИ-специфические заверения о характеристиках продукта, важно давать такие заверения исключительно о фактах, которые предварительно должны быть им протестированы и зафиксированы, но не об основаниях и причинах каких-либо отклонений от этих фактов в прошлом или будущем или наступлении связанных с этим последствий, как это нередко включают в «традиционные» заверения.

3.5.2 Раскрытие информации

Продавцам ИИ-компаний следует уделить особое внимание процедуре раскрытия информации (disclosure). В первую очередь это необходимо для балансирования объема ответственности по заверениям, которые может запросить покупатель в отношении ИИ-активов. Еще одной причиной является законодательно установленная обязанность сторон сделки действовать добросовестно, в том числе предоставлять друг другу информацию, значимую для принятия ими обязательств по сделке (т. н. стандарт объективной добросовестности).

Какую важную информацию, помимо той, которая касается юридических аспектов, разработчик ИИ-системы может раскрыть покупателю в отношении ИИ-активов, а тот — ожидаемо запросит предоставление таких сведений? Важно понимать, что разработчик ИИ-системы не обязан раскрывать покупателю информацию об используемой ИИ-технологии (в первую очередь, это касается данных, на которых обучалась базовая модель, ее архитектуры, алгоритмов обучения), **к которой у него нет и не может быть доступа**. Но он может и должен иметь документированную информацию, описывающую процесс и основные параметры интеграции, адаптации и тестирования ИИ-модели при создании и эксплуатации ИИ-системы, и обязан раскрыть ее покупателю.

К сведениям, которые целесообразно раскрыть покупателю, относятся, в частности:

- текущая стадия жизненного цикла ИИ-модели, использованная в прикладном решении;
- версия модели, описание ее архитектуры и гиперпараметров (если есть);
- необходимость или рекомендации по обновлению модели с указанием периодичности;
- описание рисков, возникающих в случае несвоевременного обновления модели;
- описание сред дообучения модели;
- характеристики вычислительных мощностей, используемых для обучения моделей;
- бенчмарки производительности и показатели скорости дрейфа модели (Accuracy, F1, Recall), определенные на тестовом датасете, прогнозы частоты дообучения модели и падения точности;
- триггеры необходимости переобучения модели (PSI, SCI);
- история инцидентов;
- наличие технического долга по обучающим данным;
- скорость инференса под нагрузкой;
- время на переобучение с момента обнаружения дрейфа;
- риски изменения поведения модели на новых обучающих данных (их категориях и типах);
- цели и задачи, для которых создан ИИ-сервис, а также иные цели, для которых его можно и нельзя использовать с учетом уточнения цели покупателя;
- все итерации дообучения модели, проведенного непосредственно под контролем оператора системы (приобретаемой компании) с указанием источника данных.

Продавцу целесообразно раскрыть покупателю эти сведения даже тогда, когда покупатель не будет запрашивать соответствующие заверения. Это необходимо для оценки покупателем технических и операционных рисков приобретаемого бизнеса, понимания динамики возможных технологических изменений, критичных для нормального функционирования сервиса. К примеру, если используемая ИИ-модель обновляется ее разработчиком с определенной периодичностью, об этом важно уведомить покупателя, как и о необходимости отслеживать процесс бета-тестирования новой версии модели, чтобы он мог своевременно перенастроить сервис под такую версию.

Также такое раскрытие информации важно, среди прочего, для целей снижения вероятности предъявления к продавцу в будущем требований, в том числе об оспаривании сделки, мотивированных возможным умышленным сокрытием значимых сведений или неумышленным введением в заблуждение в отношении характеристик ИИ-активов. Например, такой риск существует, если ряд тестов, проведенных продавцом (оператором системы) на наборе данных, имеющих явный отличительный признак (географический регион, новая целевая аудитория и т. п.), выявит необъяснимые или существенные отклонения в точности или безопасности ответов модели, но продавец не сообщит об этом покупателю.

Продавцу ИИ-компании следует раскрыть покупателю информацию, описывающую процессы интеграции, адаптации и тестирования сторонней ИИ-модели, используемой в прикладном решении, а также ключевые метрики ее поведения и динамику их наблюдений. Это важно для балансирования ответственности по заверениям, а также для снижения риска предъявления к нему требований, мотивированных возможным сокрытием значимой информации или введением контрагента по сделке в заблуждение.

Многие из таких данных есть в публичном доступе — их может раскрывать непосредственно разработчик модели. Поэтому стандарт осмотрительности покупателя высокорискового бизнеса в данном случае будет требовать самостоятельного изучения всех значимых сведений, которые могут относиться к базовой модели и ее обучающим данным. Даже если продавец не предоставит такую информацию по запросу или предоставит ее лишь частично, покупателю следует проверить соответствующие публичные ресурсы как для целей соблюдения стандарта осмотрительности на случай спора по заверениям, так и для формирования полноценной картины рисков и определения стоимости компании.



Анатолий Земцов

управляющий партнер

dfcenter

Продавец, использующий чужую модель без доступа к ее обучающим данным и внутреннему пайплайну, как правило, не располагает информацией о составе датасета, процедуре предобучения и внутренних метриках. Однако он может раскрывать (а) публичные характеристики модели (архитектура, число параметров, формат весов, заявленные метрики) и (б) результаты собственного тестирования.

Коммерческая ценность при этом формируется на уровне прикладной системы: ее тонкая настройка (если проводилась), промпт-архитектура, RAG, интеграции, инфраструктура, SLA, мониторинг, логирование и процедуры обновления. Именно этот слой находится в зоне контроля продавца и может быть предметом его гарантий при продаже бизнеса.

3.5.3 Аспекты на стороне покупателя

При запросе заверений у продавца в отношении ИИ-компании покупателю также целесообразно руководствоваться критерием подконтрольности соответствующих аспектов вопросов продавцу (оператору системы). По тем аспектам, в отношении которых у продавца полностью отсутствует контроль, запрашивать средства защиты не стоит, такой риск покупателю следует принять. Прежде всего это касается вопросов юридической «чистоты» датасетов, на которых обучалась модель до того, как ее начал использовать оператор системы.

Значительная часть рисков ИИ-системы лежит за пределами контроля продавца — на уровне базовой модели, ее обучающих данных, архитектурных ограничений и вероятностной природы ответов. Продавец не может ни проверить, ни гарантировать отсутствие таких рисков.

Сегодня транзакционные команды еще придерживаются традиционного переговорного подхода, подчиняющегося следующей логике: если покупатель не смог проанализировать риски, например из-за того, что компания не предоставила ему соответствующую информацию, — значит, он может полагаться на заверения продавца.

Однако важно учитывать, что продавец не предоставил запрошенную информацию не потому, что не захотел, а потому, что сам не располагает ею и не имеет возможности ее получить. Более того, зачастую та информация, которой обладают продавец и компания, также доступна и для покупателя, так как такие сведения являются открытыми для широкого доступа. Это означает, что покупатель имел реальную возможность проверить такую информацию сам, в том числе путем проведения технической экспертизы. Знания о соответствующих рисках или ограничениях, которые могли быть получены из открытых источников в отношении базовой модели, в случае судебного спора с высокой степенью вероятности будут вменены покупателю, что затруднит взыскание компенсации с продавца в связи с нарушенными заверениями.

Покупателю также следует помнить, что проведение технической экспертизы при приобретении ИИ-компании даже в формате black-box, без доступа к внутреннему устройству ИИ-технологии, может дать ответы о фактическом состоянии и перспективах функционирования сервиса на ближайшем горизонте.

В частности, без доступа к «начинке» базовой модели можно проверить следующие параметры, значимые для оценки работоспособности, качества и наличия технических рисков у ИИ-решения:

Функциональную точность модели	— соответствие ответов ожидаемым на примере типовых задач сервиса.
«Галлюцинации»	— выдача моделью фактов, не соответствующих действительности или заданному контексту.

Дрейф (дрифт) данных / признака / концепции — изменение поведения модели по сравнению и с более ранним периодом и «шаг» таких изменений.

Устойчивость — реакция модели на нестандартные, провокационные или зашумленные входы.

Алгоритмические смещения — систематические искажения ответов, дискриминирующие по определенным признакам.

Безопасность — способность модели нарушить заложенные в ней ограничения и фильтры (дать вредный совет, раскрыть системный промпт и т. п.).

и ряд других. Поэтому если покупатель не проведет техническую экспертизу, у него могут возникнуть сложности при доказывании своих доводов, мотивированных тем, что у него отсутствовали соответствующие сведения на момент заключения сделки по причине непредставления / нераскрытия их покупателем.

3.6 Распределение специфических ИИ-рисков

Покупатель может настаивать на распределении исторических рисков приобретаемого ИИ-актива, связанных не только с юридическими, но и с техническими, этическими и ИБ-последствиями. В ряде случаев такие требования звучат обоснованно — покупателю важно понимать, чего ожидать от приобретаемого ИИ-сервиса в ближайшем будущем, насколько он управляем, какие расходы и предпосылки, связанные с его развитием и поддержанием, следует закладывать в финансовую модель. К таким аспектам относятся уже упомянутые выше явления дрейфа, алгоритмических смещений, непрозрачности (необъяснимости), уязвимости к атакам и промпт-инъекциям, «галлюцинации» и т. п.

Вполне ожидаемо, что покупатель может запросить у продавца заверения или иные инструменты защиты от материализации таких рисков, гарантии достоверности текущих параметров соответствующих метрик, информацию о возможных отклонениях и значимых факторах влияния на их динамику, в особенности если таковые были выявлены оператором системы эмпирически на собственных тестах.

При работе с такими вопросами продавцу следует помнить, что на определенные характеристики поведения модели, интегрированной в систему, **могут влиять сразу несколько факторов, а ответственность за причины и последствия таких проявлений могут нести одновременно разные субъекты — разработчик модели, все предыдущие операторы системы** (если текущий оператор ИИ-системы приобрел такой бизнес, а не создавал его «с нуля»), **текущий оператор** (в нашем примере — продавец по сделке M&A) и **новый оператор** (покупатель). Более того, в некоторых случаях ответственность за причину инцидента несет один субъект, а за последствия — другой, или она «делится» между ними.

Поскольку некоторые специфические риски продавец (оператор системы) не контролирует или контролирует условно, а другие — существенно выше (например, дрейф данных он может контролировать меньше, чем алгоритмическую предвзятость, и еще меньше, чем «галлюцинации», но многократно больше, чем «необъяснимость», которую он практически не может контролировать), — **заверения не являются подходящим инструментом для распределения таких рисков**. Для этого больше подходит механизм возмещения имущественных потерь или отложенного обусловленного платежа (удержание части цены). Однако заверения могут быть эффективно использованы для целей:

- **описания мероприятий**, которые оператор ИИ-системы фактически предпринял для того, чтобы предотвратить негативные сценарии проявления указанных исков, например дрейфа;
- **фиксации ключевых метрик**, характеризующих степень соответствующего риска, (например, величину или порог метрик PSI или F1-score при описании дрейфа);
- подтверждение факта **внедрения в компании конкретных политик и процедур** в качестве локальных актов, регламентирующих процессы измерения и мониторинга соответствующих показателей.

Мы попросили экспертов на примере явления дрейфа рассказать, как стороны могут распределить такой риск с помощью транзакционных инструментов и как его выявить с помощью технической экспертизы.



Софья Смирнова

советник M&A
и корпоративной практики

O_2 консалтинг

Отдельно стоит упомянуть распределение такого риска, имманентно присущего ИИ-моделям, как дрейф (дрифт) моделей. Так, поскольку ИИ-модели с течением времени деградируют (т. н. дрейф (дрифт) ML-моделей), владельцы моделей разумно обеспечивают защиту от дрифта специальными мерами (мониторинг качества, переобучение на новых данных и т. п.). И такие заверения о принятии мер необходимо включать в документацию по сделке. В случае с ИИ-бизнесами, построенными на API чужой ИИ-модели, такие меры, если анализ выдачи и ведется, не влияют на модель, и поэтому продукт очевидно построен на «доверии» к поставщику фундаментальной модели, инвестирующего большие средства и человеческие ресурсы в контроль и комплаенс. В случае, когда продукт строится на чужой опенсорсной модели, на наш взгляд, именно продавец должен обеспечить защиту от дрейфа (или хотя бы порядок замены модели на другую).

Как должны выглядеть заверения и возмещения имущественных потерь касательно дрифта моделей? Во-первых, следует обязательно указывать понятное технической команде предельное значение дрейфа (проще всего — усредненный % дрейфа в определенный период), выше которого должно наступать возмещение (состоящее преимущественно в расходах на переобучение модели для устранения дрейфа, а также убытки за простой бизнеса на этот период). При этом доказывание факта наступления дрейфа по причинам, имевшим место до сделки, является на практике крайне затруднительным. Крайне важны формулировки заверения или условия возмещения потерь — поскольку именно в них будет крыться то, что именно должен будет доказать покупатель (что случилось, когда это случилось, почему это произошло, что именно за это продавец обязался отвечать). Поэтому с точки зрения механизмов защиты интересов покупателя лучше выбирать механизм возмещения потерь на случай возникновения дрейфа, а в заверения включать, что модель на дату закрытия соответствует определенным метрикам (с детализацией того, как они посчитаны) и в обществе приняты все необходимые меры для своевременного

обнаружения дрейфа, а также проведена аналитика, на каких данных ИИ-модель работает хуже или лучше (то есть произведена полноценная подготовка к устранению дрейфа). Размер возмещения также очень трудно оценить заранее — в силу уникальности и дороговизны компетенций и данных, необходимых для устранения дрейфа (а иногда и невозможности его устранения в некоторых случаях), размер возмещения может колебаться от заниженного до стоимости всего бизнеса. Наконец, метрика в % дрейфа также может являться не вполне релевантной для кейса, когда дрейф произошел не в том графике, который ожидала техническая команда покупателя, и / или в отдельных областях (для определенных данных) процент дрейфа оказался выше, и это стоило компании дороже, чем небольшой дрейф в других областях. Все сценарии предусмотреть, скорее всего, будет невозможно — поэтому на текущей стадии зрелости большинства продуктов (если мы не говорим об инвестициях в бигтех) допустимо брать усредненные значения, принимая во внимание раннюю стадию развития рынка.

Приведем пример. Продавец разрабатывает систему скоринга юридических рисков договоров, обученную на практике судов преимущественно одного региона (например, московского). Продавец не раскрыл покупателю, что региональные суды (в силу специфики находящихся там предприятий и их отношений с контрагентами, а также иных причин) выносят несколько другие решения, и Population Stability Index (метрика дрейфа) на таких данных выше, чем на обучающей выборке, и F1-score (еще одна метрика дрейфа) соответственно ниже. При развитии продукта F1 закономерно упала, результаты стали неточными. Покупатель будет доказывать, что отклонение метрик существовало или было предвидимо на дату закрытия, продавец же будет доказывать, что это произошло вследствие изменения аудитории продукта или решений покупателя. Если результаты замеров (метрики) достаточно хорошо не задокументированы по итогам ДД (с приложением всех данных), разумно назначаемая судом техническая экспертиза не сможет подтвердить позицию покупателя,

и возмещение он не получит. Поэтому разумно не только очень внимательно документировать такие замеры, но и забирать с продуктом его изначальный обучающий датасет (даже если он устарел) и делать прозрачные замеры в течение определенного периода после сделки, чтобы найти основание ответственности продавца. Если же дрейф все же случится при условии, что покупатель все документировал и нормально эксплуатировал ИИ-модель, и причины этого существовали до даты сделки (например, скрытый дефект в данных или технический долг выбранной архитектуры), то продавец должен возместить, как минимум, расходы покупателя на переобучение, создание новых датасетов, предвидимые убытки от некорректной выдачи (при наличии).

При сильной позиции покупателя также разумно устанавливать удержание части покупной цены / механизм earn-out, чтобы смягчить влияние всех вышеуказанных факторов на сделку.



Анатолий Земцов

управляющий партнер

dfcenter

@DFC_BLOG →

Предположим, что стратег купил ИИ-стартап с сервисом, построенным поверх ChatGPT. Суть сервиса — бот для кол-центра, обращающийся к базе знаний и отвечающий на самые распространенные запросы пользователей. Покупатель провел дообучение на своей базе Q&A — для ускорения онбординга новых масснаборных сотрудников (т. е. не внешних клиентов). У бота существенно возросло количество неверных / неадекватных ответов. В отношении дрейфа продавец давал заверение или обязался возместить потери в случае, если параметры дрейфа превысят те, что были согласованы сторонами. Покупатель предъявляет претензии продавцу, потому как уверен, что произошел «дрейф данных».

1. Чтобы обоснованно говорить о дрейфе или об ошибках вообще, необходимо провести экспертизу и выяснить, в чем конкретно заключаются ошибки и что было их причиной. Для этого в ряде случаев достаточно сделать тестовые запросы сервису и проанализировать ответы.

   Помимо прочего экспертиза покажет, где локализована проблема: на уровне бот-сервиса или на уровне базовой модели (за которую продавец вообще не отвечает).

2. Чтобы говорить о дрейфе выше определенного показателя или вообще дрейфе как таковом, нужно знать, какие допустимые пределы ошибок имела система в момент продажи, а какие фактические показатели есть сейчас. Действительно ли есть изменения и какие. Для того чтобы гарантированно знать параметры прошлого при передаче сервиса покупателю, продавцу необходимо (было) максимально подробно зафиксировать технические параметры передаваемого сервиса.
3. Текущее значение ошибок, а также их причина, будут установлены в п. 1. Это может быть как проблема бот-сервиса, так и сбои в базовой модели (за которые продавец не отвечает). Конкретно же в описанной ситуации это «вина» самого покупателя, неверно проведшего процесс дообучения. Все это будет выявлено при исследовании сервиса.

3.7 Прочие инструменты распределения рисков

3.7.1 Возмещение имущественных потерь

Инструментарий заверений (ст. 431.2 ГК РФ) связан с рядом ограничений, не позволяющих сторонам сделки эффективно распределить риски. В первую очередь, к ним относится **высокий стандарт должной осмотрительности покупателя**, из-за несоблюдения которого суд может отказать в компенсации убытков по гарантиям даже в менее рисковых сделках (с ростом риска повышается стандарт осмотрительности), а также **практическая невозможность реализации гарантий по аспектам, которые продавец не контролирует**.

Если переговорная позиция продавца более слабая, он может согласиться прогарантировать покупателю обстоятельства, за которые он не отвечает и не влияет на них. В этом случае он столкнется с доктринальной проблемой невозможности гарантировать «чужое поведение» и риском заведомо ложных заверений. А покупателю в такой ситуации будет крайне сложно доказать причинно-следственную связь при обосновании убытков. Поэтому если продавец все же согласен отвечать за действия третьих лиц, в том числе тех, которые он никак не контролирует, **стороны могут применить более «сильный» инструмент — возмещение имущественных потерь**.

> **Доказать, что какие-либо технические или этические риски ИИ-продукта материализовались после закрытия сделки по причинам, возникшим до даты ее закрытия, — крайне сложно.**

> **Тщательное документирование соответствующих метрик на дату подписания или закрытия сделки необходимо, — это позволит установить факт наступления триггера для компенсации и понять, отклонились ли метрики в худшую сторону от заявленных. Но этого недостаточно для определения первопричины произошедших изменений, а также для установления периода, в котором они возникли.**

В этом случае пределы возможностей сторон по распределению ИИ-специфических рисков расширяются — **продавец может обязаться компенсировать имущественные потери, которые возникли, например, на уровне базовой модели**, за который отвечает разработчик модели. К такого рода рискам, которые могли бы быть «закрыты» имущественными потерями, относятся также риски дрейфа, алгоритмической предвзятости и даже «непрозрачности» (необъяснимости) ответов модели, хотя этот риск, в отличие от двух ранее упомянутых, полностью находится вне контроля оператора системы.



Софья Смирнова

советник M&A
и корпоративной практики

O_2 консалтинг

Если ИИ-бизнесы (в особенности с чужой проприетарной моделью) несут в себе риски, то эти риски необходимо перераспределять документацией. При этом сам факт того, что заверения могут быть недоступны в некоторых сценариях, не значит, что риски нельзя распределять. Соответственно, сильный покупатель включит в документацию возмещение потерь на случай выявления отдельных связанных с бизнесом обстоятельств, за которые в том числе не отвечает продавец, но которые влияют на оценку бизнеса (и его финансовые показатели). Эти обстоятельства так или иначе вытекают из самой сути лежащей в его основе сложнейшей технологии. При этом многослойность ИИ-бизнесов, в которых чаще всего будут присутствовать те или иные чужие компоненты (крайне мало бизнесов способны на полностью автономную разработку конкурентных полностью собственных ИИ-продуктов), влечет постановку вопроса, как такие риски справедливо и разумно было бы распределять между продавцом и покупателем.

В качестве оснований для возмещения потерь (ст. 406.1 ГК РФ) покупателем могут включаться в документацию следующие обстоятельства:

1. Предъявление обществу третьим лицом претензии или иска, связанных с контентом, сгенерированным ИИ-системой до даты закрытия, а также, при сильной позиции покупателя, для ИИ-продукта на основе чужой базовой модели, на основе данных, использованных обществом для создания продукта до даты закрытия, в том числе по основаниям нарушения авторских и смежных прав, прав на изображение гражданина, прав на защиту чести, достоинства и деловой репутации, прав субъектов персональных данных.
2. Предъявление обществу уполномоченным регулятором предписания, акта о привлечении к ответственности или иного аналогичного решения, основания применения которого возникли до даты закрытия.

3. Расторжение или приостановление провайдером базовой модели договора с ним, прекращение или существенное ограничение доступа общества к базовой модели, основания применения которых сложились до даты закрытия, в том числе в связи с ретроспективно установленными нарушениями условий использования (как элемент титульной гарантии).
4. Применение к обществу санкционных, экспортных или иных ограничивающих мер, делающих использование базовой модели невозможным или существенно более затруднительным, при условии, что юридические основания применения таких мер сложились до даты закрытия (с соответствующим раскрытием системы прокси-доступа к ИИ-моделям из недружественных стран).
5. Утечка персональных данных или иных конфиденциальных сведений, обрабатываемых Обществом, при условии, что причины утечки сформировались до даты закрытия.
6. Выявление систематических дефектов ИИ-системы (включая систематические галлюцинации в критически значимых сценариях использования и скрытую предвзятость, а также дрейф (дрифт) модели), причины возникновения которых имели место до даты закрытия.

Для ИИ-бизнесов, основанных на чужих базовых моделях, видится разумным принцип принятия на себя всех рисков, связанных с состоянием чужой базовой модели, именно покупателем такого бизнеса (например, п. 1 и 6), поскольку данный бизнес является очевидно высокорискованным, а также потому что продавец в принципе не способен влиять на базовую модель и создает добавленную ценность вокруг нее (не получая, в свою очередь, от владельца модели в подавляющем большинстве случаев каких-либо гарантий). Тем не менее, лучших практик на рынке пока что не сложилось, и в зависимости от наличия в цене сделки «премии» за скорость входа на рынок может так получиться, что продавец возьмет на себя определенные обязательства по возмещению потерь в случае обстоятельств, за которые объективно не мог бы отвечать.

О чем важно помнить сторонам при применении инструмента возмещения имущественных потерь для целей распределения ИИ-рисков

Во-первых

- Следует очень аккуратно прописывать основание-триггер возмещения потерь, особенно если речь идет о технических параметрах поведения модели. В этом случае необходима не только **фиксация метрик** на дату заключения или закрытия сделки (чего было бы достаточно для инструментария заверений), но и **понимание их динамики**, чтобы правильно указать пределы значений, выход за которые в определенный период времени будет считаться основанием для компенсации.

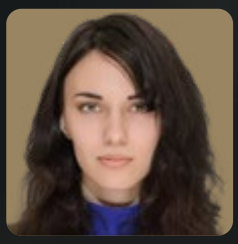
Во-вторых

- Важно помнить, что, используя такой инструмент, стороны могут договориться **о любом ретроспективном периоде**, к которому могут относиться первопричины возникновения имущественных потерь, возникших после даты закрытия сделки. Это может быть как период владения бизнесом продавцом до его передачи покупателю, так и более ранний период, имеющий естественные ограничения (выпуск соответствующей модели на рынок и т. п.). Чаще всего стороны выбирают **разумный подход** и ограничивают период возникновения причины, приведшей к имущественным потерям после закрытия сделки, **периодом владения бизнеса продавцом в пределах общего срока исковой давности**.

В-третьих

- В рамках инструментария возмещения имущественных потерь основанием их компенсации может быть событие, **полностью находящееся вне контроля продавца**. Однако это не обязательно, и в ряде случаев стороны регулируют этим механизмом обстоятельства возмещения, причины которых прямо или косвенно подконтрольны продавцу. При этом важно, чтобы такие потери **не были результатом прямого нарушения продавцом договора**, стороной которого является покупатель, поскольку этот механизм не является упрощенным способом возмещения убытков за нарушение обязательств.

Покупателю следует учитывать, что при реализации механизма возмещения имущественных потерь ему придется обосновать наличие и размер потерь, причинно-следственную связь между событием-триггером и потерями. Применительно к ряду проявлений технических или этических рисков модели (например, дрейфа) **покупателю будет крайне сложно доказать, что причина согласованных метрик дрейфа, например скорости, относится к периоду владения бизнеса продавцом**. Если условием возмещения потерь будет событие, причина которого возникла в период до закрытия сделки, и при этом зависела от поведения продавца, — пройти этот фильтр будет еще сложнее. На поведение модели (например, проявления дрейфа) к моменту подачи покупателем иска после сделки будет влиять больше факторов, чем до сделки, начиная от управления моделью разработчиком в течение всего периода времени, заканчивая собственными действиями нового оператора системы (покупателя).



Анастасия Нерчинская

Реализация механизма возмещения имущественных потерь в отношении специфических ИИ-рисков сложна и не имеет линейной логики. Недостаточно просто написать в договоре положение о том, что, если такая-то метрика, например, характеризующая степень дрейфа или алгоритмической предвзятости, в течение такого-то срока отклонится от согласованных пределов, продавец обязуется возместить покупателю все имущественные потери, если основания такого отклонения возникли до даты закрытия сделки. Важно понимать следующее:

- У имущественных потерь, связанных с ИИ-рисками (например, с дрейфом), как и у триггеров их реализации (например, претензий пользователей или требований регулятора), может быть **одновременно несколько первопричин**, атрибутируемых разным субъектам ответственности: вендору (разработчику) модели, продавцу (предыдущему оператору системы), покупателю (текущему оператору системы). Проблема могла возникнуть в результате наложения таких причин друг на друга, при этом **степень влияния каждой из них на возникновение потерь может быть очень разной**.
- Потери (на том же примере дрейфа) в размере стоимости, о которой заявляет покупатель, могли возникнуть в результате стечения нескольких причин, включая **естественные** (например, дрейф соответствует «нормальной» скорости деградации модели) или **случайные** (например, из-за макроэкономических причин резко изменилось поведение клиентов ИИ-сервиса). Либо потери имеют очень **отдаленную причинно-следственную** связь с первопричиной. Например, из-за действий продавца после закрытия сделки усилилась алгоритмическая предвзятость, которая и повлияла на точность ответов, при этом степень дрейфа не изменилась бы так сильно, если бы не действие первого фактора).
- Иск к продавцу о возмещении имущественных потерь, с учетом сроков просуживания, может быть предъявлен через несколько лет после закры-

тия сделки. Важно в течение «открытого» периода предъявления претензий обеспечить сохранность логов ключевых артефактов, которые могут быть использованы в качестве доказательственной базы в рамках спора.

Таким образом, чтобы управлять специфическим ИИ-риском через механизм распределения имущественных потерь, недостаточно отслеживать динамику какой-либо одной ключевой метрики, указанной в условии триггера компенсации. В транзакционной документации целесообразно согласовать (если контекст условия о возмещении потерь это допускает), какую информацию или доступ к каким данным, системам, журналам логирования, обучающим выборкам, включая тестовые, продавец обязан передать покупателю или обеспечить их физическую сохранность до и после закрытия сделки и какое содействие технического характера должен оказать покупателю в случае возникновения спора. Это особенно важно, если условия сделки не предполагают сохранение команды или есть высокая вероятность ее смены после закрытия сделки.

3.7.2 Отложенный обусловленный платеж

Если покупатель ИИ-бизнеса обладает более сильной переговорной позицией, он с высокой вероятностью будет настаивать на применении механики обусловленного отложенного платежа для митигации исторических рисков. Здесь работает такой же принцип, что и в рамках применения механизма возмещения имущественных потерь. То есть в качестве условия выплаты покупателю части цены можно указать отсутствие в течение определенного периода фактов материализации рисков, **в том числе тех, которые продавец никак не контролирует**. Однако такой подход в отношении некоторых рисков не представляется разумным, поскольку на этапе его реализации покупатель столкнется с теми же сложностями, что и в рамках применения инструмента возмещения имущественных потерь. Поэтому в большинстве случаев целесообразно использовать такой механизм «страховки» от исторических рисков **в отношении вопросов, разумно контролируемых продавцом**.

Почему это так? Механизм отложенного обусловленного платежа, который периодически путают с механикой earn-out, экономически имеет те же самые цели, что и механизм возмещения имущественных потерь. **Он защищает покупателя от материализации исторических рисков. Механика отложенного платежа направлена не на обеспечение роста стоимости или эффективности бизнеса**, а на его защиту от размытия (утечек) текущей стоимости, в отношении величины которой у сторон сделки нет разногласий.

Условием выплаты части платежа является отсутствие (или непроявление) в течение оговоренного срока скрытых дефектов ИИ-актива. Они нередко привязаны к техническим показателям, которые требуют **четкой объективации и верификации**. Поэтому сторонам следует обеспечить измерение соответствующих метрик на тестовом наборе данных или подтверждение их значений и характеристик независимым техническим экспертом. Для покупателя особое значение приобретает наличие у компании системы управления такими метриками. В случае спора он должен будет доказать факт срабатывания триггера компенсации (материализации риска), для чего ему понадобится доступ к соответствующим данным.

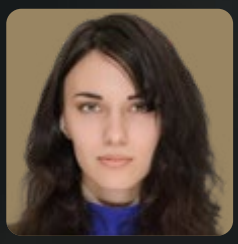
Почему такой механизм, несмотря на кажущуюся простоту для покупателя, — сложен и не всегда предсказуем? Реализация механики платежа под условием предполагает, что часть изначально понятной цены (что отличает механику от earn-out) откладывается в escrow или остается в распоряжении покупателя при наличии у него сильной переговорной позиции.

С наступлением триггера покупатель вправе недоплатить — удержать соответствующую часть, на которую уменьшается цена. Он заинтересован в том, чтобы использовать инструмент зачета встречных требований, который позволит прекратить взаимные обязательства сторон. Однако для этого триггер выплаты оставшейся части цены должен быть сформулирован не как условие, а как некое обязательство продавца, сумма которого, в случае его нарушения, могла бы быть зачтена против обязательства покупателя выплатить часть «удерживаемой» цены. Но такое обязательство довольно сложно сформулировать, особенно в части рисков, отдаленно подконтрольных продавцу. К тому же редкий продавец согласится на автоматический зачет требований, прекращающий взаимные обязательства. Это означало бы фактическое право покупателя на одностороннее уменьшение цены, поскольку продавцу будет крайне сложно оспорить в суде зачет, на который он заранее согласился.

Поэтому наиболее распространена практика, когда обязательству покупателя выплатить оставшуюся часть цены **противопоставляется обязательство продавца возместить покупателю убытки в результате нарушения заверений или сумму имущественных потерь**. А такие обстоятельства в соответствии с рыночной практикой практически всегда требуют предварительного просуживания как минимум до вынесения решения судом апелляционной инстанции. Сумму, которую суд присудит покупателю по иску о нарушенных гарантиях или возмещению потерь, **стороны зачастую договариваются «зачесть» против удержанной части цены**. В этом случае покупателю на первом этапе будет необходимо просудить имущественные потери, а значит — он неизбежно столкнется с теми же сложностями процессуального характера (см. выше).

> **Earn-out работает «вправо» (продавец может «дозаработать» дополнительную цену), а «классический» отложенный платеж — в обе стороны. Обе механики направлены на урегулирование разнонаправленных целей, поэтому часто они совмещаются в рамках единой структуры сделки. К сделкам с ИИ-активами это относится в полной мере.**

Вопросы, лежащие в основе спора продавца и покупателя в отношении исторических рисков, могут затрагивать технические аспекты функционирования ИИ-системы, исторические риски которых могут иметь разные первопричины. Поэтому при структурировании механизма обусловленного отложенного платежа, связанного с историческими рисками, обеим сторонам важно заранее продумать, как они обеспечат доказательственную базу и будут ли иметь доступ к соответствующим метрикам в случае спора.



Анастасия Нерчинская

@SDELKIMNA →

M&A I AI →

Отложенный обусловленный платеж фактически используется не как удобная конструкция, позволяющая покупателю автоматически (без решения суда) уменьшить оговоренную цену. А лишь как механизм обеспечения исполнения продавцом своих же обязательств, направленных на сохранение текущей стоимости бизнеса (нереализацию исторических рисков, включая те, которые могут повлиять на прогнозные денежные потоки, но их причины возникли до закрытия сделки).

У механики отложенного обусловленного платежа и у заверений или обязательств возместить потери часто зеркально-противоположные триггеры. Реализация конкретного риска может привести к выплате компенсации продавцом покупателю суммы убытков или потерь. А нереализация фактически того же риска — может стать основанием для выплаты покупателем продавцу оставшейся части цены. Обязательства по выплате соответствующих сумм могут быть прекращены зачетом встречных требований (достаточно волеизъявления одной из сторон) или взаимной договоренностью (прекращение обязательств соглашением сторон), заранее предусмотренной в транзакционной документации.

При использовании такой механики для «страховки» от специфических ИИ-рисков нужен доступ к системе мониторинга соответствующих технических параметров. Поэтому для покупателя спор по иску о взыскании имущественных потерь или убытков по заверениям является фактически первой и основной фазой реализации механики обусловленного отложенного платежа. Для продавца это означает, что сроки выплаты оставшейся части цены могут быть существенно затянуты, если в течение соответствующего периода покупатель инициирует суд по взысканию убытков или потерь. В этом проявляется обеспечительное свойство такой механики на стороне покупателя.

3.7.3 Earn-out

Механизм earn-out, несмотря на его сходство с «классическим» отложенным платежом под условием (первый является частным случаем второго), имеет **принципиально иное целеполагание.** Earn-out направлен на обеспечение роста стоимости ИИ-актива или улучшение показателей его эффективности, а не на защиту от исторических рисков и скрытых дефектов бизнеса. Зачастую эти цели противоположны. Рост бизнеса, особенно высокорискового, нередко достигается в ущерб его эффективности, и наоборот.

Механика отложенного платежа используется тогда, когда сторонам на дату закрытия сделки **известна и понятна стоимость всего бизнеса** (то есть величина Enterprise Value). В отношении нее отсутствует спор, стороны сделки понимают, что возможные колебания EV, в том числе в сторону увеличения, уже не будут системными. При этом участники сделки также понимают ориентировочную стоимость рисков, которые могут материализоваться и привести к уменьшению (размытию) текущей стоимости бизнеса. Главным практическим отличием механики earn-out от классического обусловленного платежа является то, что в первом случае итоговая цена известна (ее возможные колебания не принципиальны), а во втором — нет.

Сделки с ИИ-бизнесами относятся к высокорисковым, характеризующимся волатильностью показателей и значительной неопределенностью динамики выручки, темпов роста, параметров риска. Поэтому в сделках с ИИ-активами механика earn-out встречается наиболее часто, так как призвана разрешить проблему «разрыва в оценках».

Такая механика связана со **сложностью объективации метрик и параметров**, достижение которых является триггером для увеличения оценки и выплаты дополнительного вознаграждения продавцу. Это характерно не только для сделок с ИИ, но и для любых других сделок с ИТ-активами. Однако если КПЭ, в зависимость от которых поставлен earn-out, будут связаны с ИИ-метриками, сторонам также потребуется доступ к соответствующим техническим данным, как и помощь технических специалистов при формулировании соответствующих триггеров и фиксации факта достижения или недостижения КПЭ.

1

Приложение

Используемые термины

Если из контекста этого исследования прямо не следует иное, все указанные ниже слова и выражения, используемые в тексте исследования, имеют следующие значения:

АО — акционерное общество.

ГК РФ — Гражданский кодекс Российской Федерации.

ДКП или **SPA** — договор купли-продажи.

долл. — доллар США.

Законопроект Минцифры — проект федерального закона «Об основах государственного регулирования сфер применения технологий искусственного интеллекта в Российской Федерации», опубликованный Минцифры России на федеральном портале проектов нормативных актов 17 марта 2026 г., ID проекта 166424, ссылка на публикацию на портале — https://regulation.gov.ru/projects/166424/.

ЗПИФ — закрытый паевой инвестиционный фонд по смыслу Федерального закона от 29.11.2001 № 156-ФЗ «Об инвестиционных фондах».

ИБ — информационная безопасность; все выражения с приставкой «**ИБ-**» следует толковать соответственно.

ИИ или **AI** — искусственный интеллект.

ИИ-компания или **ИИ-бизнес** — бизнес, в котором ИИ-функциональность лежит в основе стоимости и является его ключевой технологической составляющей, без которой функционирование бизнеса невозможно.

ИС или **IP** — интеллектуальная собственность.

ИТ или **IT** — информационные технологии.

КИИ — объект критической информационной инфраструктуры.

КД или **SHA** — корпоративный договор.

КПЭ или **KPI** — ключевые показатели эффективности.

ЛНА — локальный нормативный акт.

Минцифры — Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации.

НДС — налог на добавленную стоимость.

НДФЛ — налог на доходы физических лиц.

НК РФ — Налоговый кодекс Российской Федерации.

ООО — общество с ограниченной ответственностью.

ПДн — персональные данные.

ПО — программное обеспечение.

проверка бизнеса, или **due diligence**, или **DD** — финансовая, налоговая, юридическая, техническая или иная проверка бизнеса (в зависимости от контекста).

РИД — результат интеллектуальной деятельности.

Роскомнадзор — Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Роспатент — Федеральная служба по интеллектуальной собственности Российской Федерации.

РРПО — Единый реестр российский программ для электронных вычислительных машин и баз данных.

руб. — законная валюта Российской Федерации.

СП — совместное предприятие.

СУБД — система управления базами данных.

СХД — система хранения данных.

таргет — приобретаемая в рамках сделки M&A компания, бизнес, группа компаний.

ФСТЭК — Федеральная служба по техническому и экспортному контролю Российской Федерации.

ФСБ — Федеральная служба безопасности Российской Федерации.

ЦОД — центр обработки данных.

API или **Application Programming Interface** — интерфейс программирования приложений.

ARR или **Annual Recurring Revenue** — годовая возобновляемая (регулярная) выручка.

asset-deal — тип сделки, при котором покупатель приобретает конкретные активы целевой компании, а не ее акции или доли в уставном капитале.

cash-in или **сделка cash-in** — сделка по внесению вклада в уставный и / или добавочный капитал компании, в результате которой происходит изменение структуры и величины акционерного капитала (equity).

cash-out или **сделка cash-out** — сделка купли-продажи актива, долей или акций, стоимость которых покупатель выплачивает продавцу, и которая не приводит к изменению величины акционерного капитала (equity) компании.

churn или **churn rate** — коэффициент оттока клиентов, маркетинговая метрика, которая отражает долю потребителей, прекративших взаимодействие с продуктом (отписавшихся от сервиса, переставших совершать покупки, расторгнувших договор и т. д.) за конкретный промежуток времени.

completion accounts — механика корректировки покупной цены, при использовании которой величины чистого долга и чистого оборотного капитала определяются на основе отчетности приобретаемой компании, составленной на дату закрытия сделки.

Earn-out — механика расчетов, при которой на этапе закрытия сделки выплачивается согласованная сторонами основная часть возможной покупной цены, а в случае достижения определенных сторонами КПЭ, в будущем выплачивается дополнительная часть покупной цены.

EBITDA — прибыль до вычета процентов, налогов и амортизации (англ. — Earnings Before Interest Tax Depreciation and Amortisation).

EBIT — прибыль до вычета процентов, налогов (англ. — Earnings Before Interest and Tax).

Enterprise Value или **EV** — стоимость бизнеса.

equity — акционерный капитал; все производные выражения, включая «equity-инвестиции» и «equity-инвестор», должны толковаться соответственно.

Equity Value или **E** — стоимость акционерного капитала.

ESOP — Employee Stock Ownership Plan, программа акционирования ключевых работников, позволяющая при достижении определенных КПЭ получить в качестве премии часть акций или долей в уставном капитале компании.

Fine-Tuning применительно к ИИ-модели — метод ее дообучения в формате «тонкой настройки», при котором дообучение происходит на специализированном наборе данных, в результате чего изменяются все или часть весов модели, а сама модель адаптируется к решению конкретных, в том числе узкоотраслевых задач.

Full Fine-Tuning применительно к ИИ-модели — метод ее дообучения в формате «тонкой настройки», в результате которого происходит ее полное переобучение, влекущее изменение всех ее весов.

GPU или **Graphics Processing Unit** — микропроцессор, работающий с графикой.

holdback — механика удержания покупателем части цены в течение согласованного периода после закрытия сделки, которая может полно-

стью или частично не выплачиваться продавцу в случае материализации исторических рисков в пределах стоимости такого удержания.

IPO или **Initial Public Offering** — первичное публичное размещение акций.

LLM или **Large Language Model** — большая языковая модель.

locked box — механика корректировки покупной цены на величину отклонения согласованных сторонами параметров чистого долга и чистого оборотного капитала на дату оценки от фактических параметров чистого долга и оборотного капитала, рассчитанную на основе размера «утечек», допущенных продавцом или компанией в период между датой оценки и датой закрытия сделки.

LoRA или **Low-Rank Adaptation** применительно к ИИ-модели — метод ее адаптации посредством неполного дообучения с помощью использования низкоранговых матриц (адаптеров), в результате чего меняется лишь незначительная часть весов модели.

ML или **Machine Learning** — машинное обучение.

MRR или **Monthly Recurring Revenue** — ежемесячная возобновляемая (регулярная) выручка.

NDA или **Non-disclosure Agreement** — соглашение о неразглашении конфиденциальной информации.

on-premise или **on-prem** — модель распространения ПО, при которой его развертывание происходит локально — в закрытом контуре компании, а не на внешних серверах.

PE или **сделка PE** — сделка инвестирования частного капитала (или Private Equity).

PEFT или **Parameter-Efficient Fine-Tuning** применительно к ИИ-модели — ее адаптация к выполнению конкретных задач методом неполного дообучения с минимальными ресурсно-вычислительными затратами (включая метод LoRA), в результате чего меняется лишь незначительная часть весов модели.

RAG или **Retrieval-Augmented Generation** применительно к ИИ-технологиям — архитектурный подход, позволяющий расширить контекст ИИ-модели путем ее обращения к внешней базе знаний.

R&D или **Research and Development** — деятельность по разработке новых продуктов и услуг.

SaaS или **Software as a Service** — модель распространения ПО, при которой приложение развертывается на серверах поставщика услуги, а пользователи получают удаленный доступ к его функционалу без получения экземпляра ПО.

share-deal — тип сделки, при котором покупатель приобретает акции или доли в уставном капитале целевой компании.

SLA или **Services Level Agreement** — соглашение об уровне сервисного обслуживания.

SPO или **Secondary Public Offering** — вторичное публичное размещение акций.

retention — метрика, которая показывает какой процент пользователей продолжает пользоваться продуктом или услугой после первого взаимодействия с ними.

TMT — сектор технологий, медиа и телекоммуникаций.

VC или **сделка VC** — сделка инвестирования в рискованные и потенциально высокодоходные проекты, совершаемые путем приобретения доли участия в уставном капитале непубличной компании — реципиента инвестиций и / или предоставления долгового финансирования с возможностью конвертации долга в доли или акции (equity).

Метрики unit-экономики и объема рынка:

ARPPU или **Average Revenue Per Paying User** — метрика, показывающая средний доход на одного платящего пользователя за определенный период времени.

CAC или **Customer Acquisition Cost** — метрика, показывающая стоимость привлечения одного клиента.

CPA или **Cost Per Action** — метрика, показывающая стоимость одного целевого действия после того, как пользователь впервые увидел рекламу продукта.

LTV или **Lifetime Value** — метрика, показывающая суммарный доход от одного пользователя за все время его взаимодействия с продуктом.

PAM или **Potential Available Market** — метрика, показывающая потенциальный (максимально возможный) объем рынка продукта или услуги.

TAM или **Total Addressable Market** — метрика, показывающая общий объем целевого рынка, на котором можно реализовать продукт или услугу с учетом географии, барьеров рынка, платежеспособности целевой аудитории и другой специфики.

SOM или **Serviceable Obtainable Market** — метрика, показывающая реально достижимый объем рынка продукта или услуги с учетом текущей маркетинговой стратегии.

Для целей ссылки на данные онлайн опросов:

Опрос по аспектам Tech M&A — онлайн-опрос по аспектам комплексной проверки ИТ-активов, митигации рисков и структурированию сделок приобретения ИТ-компаний и / или программных продуктов и сервисов, лежащих в основе технологических бизнесов, состоящий из 22 вопросов, подробное описание которого приведено в Приложении 2 «Методология исследования».

Опрос по структурированию сделок Tech M&A в 2025 г. — онлайн-опрос по динамике Tech M&A-активности в 2025 г., сегментам и вертикалям в фокусе сделок Tech M&A, преобладающим структурам и форматам сделок, подходам к due diligence и управлению рисками, особенностям структурирования сделок, состоящий из 9 вопросов, подробное описание которого приведено в Приложении 2 «Методология исследования».

Опрос об эффективности заверений в сделках cash-in — онлайн-опрос, посвященный вопросам допустимости и эффективности включения заверений, предоставляемых инвестору в рамках сделки cash-in, в корпоративный договор, а также необходимости уведомления инвестора о рисках, связанных с неэффективностью заверений, включенных в корпоративный договор, состоящий из 2 вопросов, подробное описание которого приведено в Приложении 2 «Методология исследования».

2

Приложение

Методология исследования

1. Предмет и фокус исследования

Общий подход

Данное исследование посвящено анализу аспектов юридического структурирования, сделок с российскими непубличными компаниями сегмента TMT (сделки Tech M&A) за период с 01.01.2025 по 31.12.2025. Исследование включает детальный обзор трендов и особенностей структурирования сделок Tech M&A в 2025 г., комплексный анализ специфики переговорного процесса, вопросов due diligence программных продуктов и управления рисками, а также представляет результат углубленного изучения аспектов структурирования сделок M&A с ИИ-активами по российскому праву. Помимо результатов анализа актуальных вопросов юридического структурирования сделок Tech M&A по итогам 2025 г., в рамках исследования был обобщен и представлен многолетний опыт хедлайнеров исследования, полученный в ходе сопровождения сделок с технологическими активами.

Если контекст исследования **прямо не указывает на иное**, под сделками Tech M&A понимаются любые сделки, вне зависимости от их структуры, формата и размера приобретенного пакета участия, которые одновременно удовлетворяют следующим признакам:

- сделка совершена в отношении компании, учрежденной (или редомицилированной) и действующей в Российской Федерации;
- компания, являющаяся объектом сделки, на момент сделки имела оценку 100% бизнеса (EV) не менее 1 млн долл.;
- сделка была закрыта не позднее 31.12.2025;
- сделка совершена в любом непубличном формате — VC / PE / pre-IPO / M&A, и не включает сделки, совершенные на публичных рынках (IPO / SPO).

2. Спецпроекты

В рамках данного исследования экспертами Группы компаний Б1 был подготовлен материал в формате спецпроекта, посвященного финансовым аспектам структурирования транзакционной механики обусловленного отложенного платежа (earn-out).

Цель формата спецпроекта — фокусное освещение проблематики узких аспектов, наиболее актуальных в контексте вопросов, обсуждаемых в исследовании, отражающее точку зрения профессиональной команды специалистов в соответствующей сфере.

3. Общая методология исследования

Для целей проведения данного исследовании были использованы следующие методы:

3.1 Онлайн-анкетирование (опросы)

В ходе исследования были проведены 3 анонимных онлайн-опроса, посвященные различным аспектам сделок Tech M&A как в целом, так и специфично для 2025 г.: Опрос по аспектам Tech M&A, Опрос по структурированию сделок Tech M&A в 2025 г. и Опрос об эффективности заверений в сделках cash-in (соответственно).

Описание онлайн-опросов и их целевой аудитории приведено ниже.

Опрос по структурированию сделок Tech M&A в 2025 г.

Фокус опроса

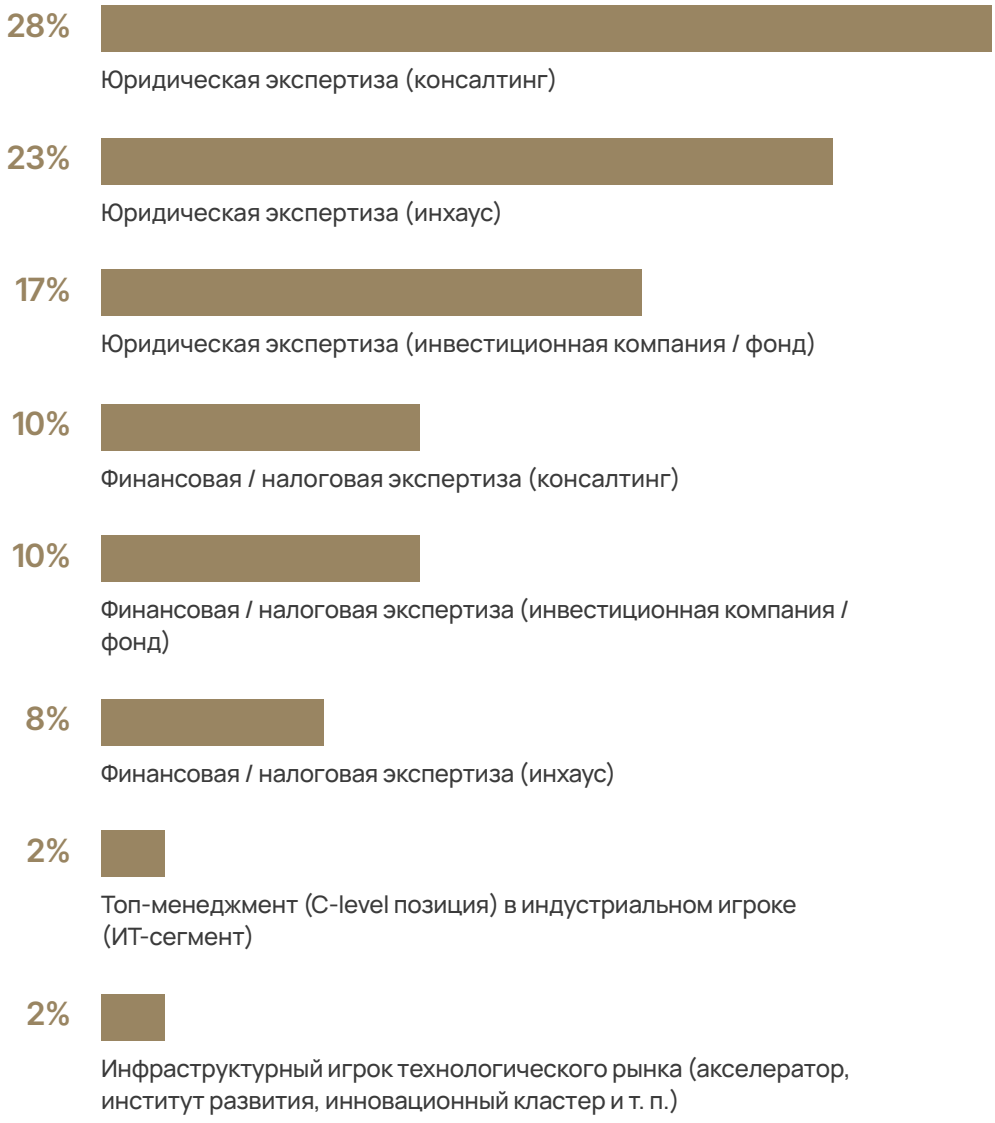
Аспекты динамики Tech M&A-активности в 2025 г., сегменты и вертикали в фокусе сделок Tech M&A, преобладающие структуры и форматы сделок в TMT в 2025 г., подходы к due diligence и управлению рисками, особенностям структурирования таких сделок.

Целевая аудитория

Юридические и финансовые консультанты, инхаус-юристы и представители финансовых и бизнес команд ИТ-компаний, технические ИТ-специалисты, которые в течение анализируемого периода принимали участие в различных форматах сделок с ИТ-бизнесами, включая ИИ-компании, или привлекались к этим процессам в качестве внешних провайдеров услуг.

Описание целевой аудитории опроса приведено на графике ниже.

Целевая аудитория опроса

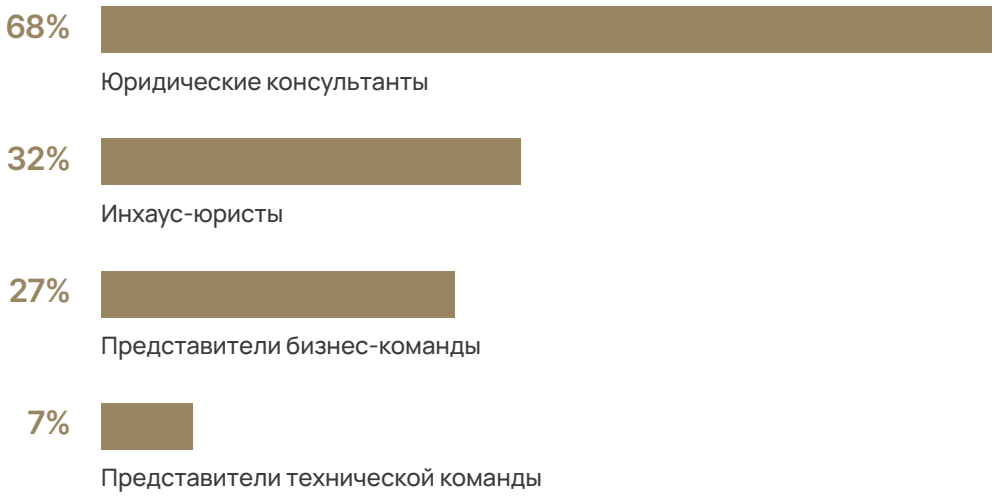


Формат	Смешанный. Большая часть ответов получена в закрытом формате — путем направления анкеты конкретным адресатам-респондентам. Остальные ответы получены путем размещения анкеты в открытом доступе, включая профильные онлайн-площадки.
Период проведения опроса	15.10.2025 г. — 30.12.2025 г.
Количество вопросов	9
Число респондентов	125

Опрос по аспектам Tech M&A

Фокус опроса	Аспекты комплексной проверки ИТ-активов (программных продуктов, баз данных), митигации рисков и структурирования сделок приобретения ИТ-компаний и / или программных продуктов и сервисов, лежащих в основе технологических бизнесов.
Целевая аудитория	Юридические и финансовые консультанты, инхаус-юристы и представители финансовых и бизнес команд ИТ-компаний, технические ИТ-специалисты, которые в течение анализируемого периода принимали участие в различных форматах сделок с ИТ-бизнесами, включая ИИ-компании, или привлекались к этим процессам в качестве внешних провайдеров услуг. Описание целевой аудитории опроса приведено на графике ниже[45].

Целевая аудитория опроса



[45] Опрос предполагал возможность нескольких вариантов ответов и фокусировался на ролях и экспертизе участия респондентов в проектах Tech M&A, в связи с чем общее число голосов превышает 100%.

Формат	Смешанный. Большая часть ответов получена в закрытом формате — путем направления анкеты конкретным адресатам-респондентам. Остальные ответы получены путем размещения анкеты в открытом доступе, включая профильные онлайн-площадки.
Период проведения опроса	27.11.2024 г. — 20.02.2025 г.
Количество вопросов	22
Число респондентов	41

Опрос об эффективности заверений в сделках cash-in

Фокус опроса	Вопросы допустимости и эффективности включения заверений, предоставляемых инвестору в рамках сделки cash-in, в корпоративный договор, а также необходимости уведомления инвестора о рисках, связанных с неэффективностью заверений, включенных в корпоративный договор.
Целевая аудитория	Юридические фирмы, принимающие участие в исследовании.
Формат	Закрытый. Все ответы получены в закрытом формате — путем направления анкеты конкретным адресатам-респондентам.
Период проведения опроса	13.05.2026 г. — 25.05.2026 г.
Количество вопросов	2
Число респондентов	48

3.2 Глубинные и блиц-интервью

В ходе исследования мы провели ряд интервью с представителями M&A- и IP / IT-команд ведущих юридических консультантов, принимающих участие в исследовании. Ответы и позиции участников интервью учитывались при формировании выводов, изложенных в исследовании.

3

Приложение

Корпоративные хедлайнеры исследования

VERBA LEGAL

VERBA LEGAL

VERBA LEGAL — российская юридическая фирма с более чем 20-летним опытом работы и обширной международной экспертизой, предоставляющая комплексное правовое сопровождение крупному бизнесу и частным клиентам.

Экспертиза и специализация

- Более 25 направлений, включая корпоративное право и M&A, международный арбитраж и трансграничные споры, фармацевтику и здравоохранение, санкционное регулирование и комплаенс и др.
- Глубокая отраслевая экспертиза: АПК и сельское хозяйство, строительство и недвижимость, транспорт и логистика, энергетика и природные ресурсы и др.

Команда и опыт

- Более 150 сотрудников VERBA LEGAL сопровождают крупнейшие регуляторные проекты «новой экономики», корпоративные сделки и прецедентные споры, в том числе трансграничные.
- 20 лет опыта по глобальным проектам в сочетании с глубоким пониманием российского права и локального рынка позволяют нам оказывать комплексную правовую поддержку и отстаивать интересы клиентов по самым сложным юридическим вопросам.
- Реализовано свыше 2500 масштабных проектов, среди клиентов — крупные российские и иностранные компании различных отраслей экономики, в том числе лидеры рейтингов Fortune Global 500, Forbes Global 2000, РБК 500 и др.

География присутствия

- Офисы представлены в Москве (Россия), Ташкенте (Узбекистан) и Мумбаи (Индия).
- Команда сопровождает проекты в более чем 30 юрисдикциях, среди которых Узбекистан, Индия, Китай (включая САО), Австрия, Бельгия, Великобритания, Германия, Ирландия, Кипр, Швейцария, Швеция, Катар, ОАЭ, Оман, офшорные юрисдикции (BVI, Каймановы острова, Сейшелы, Маврикий), Азербайджан, Казахстан, Киргизия, США, Африка и др.

Рейтинги и достижения

- Партнеры и юристы VERBA LEGAL являются признанными экспертами и отмечены престижными международными и национальными рейтингами: Chambers Global, Chambers Europe, The Legal 500 EMEA, IFLR100, Who's Who Legal, Best Lawyers, Коммерсантъ, «Эксперт-РА», Право.ru-300 и др.



Александр Панов

управляющий партнер



Александр Кузнецов

партнер



Константин Макаревич

партнер, глава практики «Инфраструктура и ГЧП»



Александр Долгов

партнер, глава практики «Инфраструктура и ГЧП»



Алексей Дарков

советник, руководитель практики «Интеллектуальная собственность»



Екатерина Третьякова

советник



Мария Мойш

старший юрист, патентный поверенный РФ



Евгения Заинчуковская

советник, руководитель практики «Налоговое и таможенное право»



Андрей Шептий

старший юрист

САЙТ VERBA LEGAL →

M&A НА ГОГОЛЕВСКОМ →

INVESTMENT ARBITRATION REVIEW →

АЛРУД

АЛРУД

АЛРУД — одна из ведущих российских юридических фирм, оказывающая все виды услуг, работающая по самым высоким стандартам по всему миру.

Наше кредо — высокое качество услуг, превосходный уровень обслуживания и строгое соблюдение этических норм.

Экспертиза и специализация

- Мы оказываем весь спектр юридических услуг в таких сферах, как корпоративное право, слияния и поглощения, антимонопольное регулирование, банки и финансы, интеллектуальная собственность, коммерческое право, защита данных / кибербезопасность, разрешение споров, уголовное право, комплаенс и расследования, иностранные инвестиции, трудовое право, реструктуризация / банкротство, недвижимость и налоги.
- С АЛРУД работают клиенты из различных отраслей, включая энергетику и природные ресурсы, горную промышленность, банки и финансы, розничную торговлю, инвестиции, государственные и общественные услуги, фармацевтику и здравоохранение, промышленность, TMT, транспортные услуги, логистику и искусственный интеллект.

Команда и опыт

- Стаж работы АЛРУД составляет более 34 лет, а ее команда насчитывает более 130 юристов. За это время АЛРУД стала одной из ведущих и снискала репутацию одной из наиболее авторитетных российских юридических фирм.
- Команда Корпоративной практики АЛРУД, которая приняла участие в ряде самых важных корпоративных сделок в разных секторах экономики и отраслях промышленности, — одна из крупнейших на российском рынке, и включает около 30 профильных юристов, которая приняла участие в ряде самых важных корпоративных сделок в разных секторах экономики и отраслях промышленности.
- Мы сопровождаем сделки любого масштаба — от частных до крупнейших трансграничных, сочетая техническую точность с пониманием стратегических целей бизнеса клиентов.

Рейтинги и достижения

Наши услуги высоко ценятся глобальным профессиональным сообществом. АЛРУД входит в международные рейтинги и удостоен наград Chambers and Partners (Chambers Global, Chambers Europe, Chambers High Net Worth, Chambers FinTech), the Legal 500, IFLR, Best Lawyers, Mergermarket, Media Law International, the Lawyer, Who is Who Legal, GCR, GAR, GIR, GDR и прочих. Одновременно с этим нашу безупречную репутацию подтверждают ведущие российские юридические рейтинги, включая ПРАВО-300, Эксперт, КоммерсантЪ.

- 1-я группа в национальном рейтинге «Право-300» в категории «Корпоративное право / Слияния и поглощения — Консультирование High-market».
- 1-я группа в национальном рейтинге «Право-300» в категории «Корпоративное право / Слияния и поглощения — Сделки M&A High-market».
- ТОП-10 юридических фирм по крупнейшим сделкам по версии Право.ru.
- 1-я группа в национальном рейтинге «КоммерсантЪ» в категории «Слияния и поглощения российских активов: High-end».
- 1-я группа в национальном рейтинге «КоммерсантЪ» в категории «Слияния и поглощения международных активов: High-end».
- 1-я группа в национальном рейтинге «Эксперты права. Лучшие юридические консультанты» в категории «Корпоративное право и сделки M&A».

Партнеры корпоративной практики АЛРУД



Александр Жарский

партнер, руководитель практики Корпоративного права и M&A сделок



Антон Джуплин

партнер



Андрей Жарский

партнер



Сергей Ханаев

партнер



Александр Клещев

партнер

САЙТ ALRUD →

КОРПОРАТИВНОЕ ПРАВО, СЛИЯНИЯ И ПОГЛОЩЕНИЯ →

DENUO

DENUO — одна из крупнейших многопрофильных юридических фирм в России. Команда DENUO обладает более чем 30-летним опытом и предоставляет своим клиентам юридические и налоговые услуги мирового уровня в рамках всех своих практик и отраслевых групп. Офисы представлены в Москве и Санкт-Петербурге (Россия), а также фирма имеет офисы в Дубае (ОАЭ), Ташкенте (Узбекистан) и Тбилиси (Грузия).

Экспертиза и специализация

- Более 25 направлений, включая корпоративное право и M&A, международный арбитраж и трансграничные споры, транспортное право, санкционное регулирование и комплаенс, и др.
- Глубокая отраслевая экспертиза: TMT, строительство и недвижимость, транспорт и логистика, фармацевтика, и др.

Команда и опыт

- Наш штат насчитывает более 100 юристов (включая 21 партнера).
- Перешедшая из DLA Piper в DENUO команда является признанным экспертом и отмечена престижными международными и национальными рейтингами: Chambers Global, Chambers Europe, The Legal 500 EMEA, IFLR100, Who's Who Legal, Best Lawyers, КоммерсантЪ, «Эксперт-РА», Право.ru-300, и др.

Рейтинги и достижения

- 2025 Лучшая юридическая фирма на венчурном рынке (Russia PE&VC Awards, PREQVECA).
- 2026 Лучшая юридическая фирма (Russia M&A Awards, PREQVECA).
- # 1 по объему сделок M&A (Mergers.ru, 2025).
- # 1 в категории Антимонопольное право (Право-300, 2022–25).
- # 1 в категории ВЭД / Таможенное право и валютное регулирование (валютное регулирование) (Право-300, 2025).
- # 1 в категории Корпоративное право / слияния и поглощения (Сделки M&A high market) (Право-300, 2022–25).
- # 1 в категории Морское право (Право-300, 2022–25).

- # 1 в категории Фармацевтика и здравоохранение (Фармацевтика) (Право-300, 2024–25).
- # 1 в категории Защита персональных данных (КоммерсантЪ, 2024–25).
- # 1 в категории Интеллектуальная собственность (Защита прав и судебные споры) (Право-300, 2022–24).
- # 1 в категории Интеллектуальная собственность (Консультирование) (Право-300, 2022–24).



Константин Лузиньян

управляющий партнер



Роман Головацкий

партнер практики интеллектуальной собственности и технологий, патентный поверенный РФ



Денис Соседкин

управляющий партнер санкт-петербургского офиса, руководитель корпоративной практики



Андрей Шиткин

партнер, руководитель практики венчурного капитала



Илья Булгаков

советник, руководитель практики защиты персональных данных



Владислав Архипов

старший советник

САЙТ DENUO.LEGAL →

ТЕЛЕГРАМ-КАНАЛ →

Advance Capital

Advance Capital — независимый инвестиционный банк в России и странах СНГ с 18-летним опытом работы, специализирующийся на сопровождении сделок по слияниям и поглощениям (покупка, продажа, объединение бизнеса), привлечении инвестиций, создании совместных предприятий, реструктуризации бизнеса, а также оказывающий сопутствующие услуги в сфере корпоративных финансов.

Специализация

Экосистема инвестиционно-банковских услуг Advance Capital позволяет закрывать все потребности наших клиентов:

M&A-консультирование (Основное направление)

- Sell-side — полное сопровождение продажи бизнеса / пакета акций.
- Buy-side — помощь в покупке активов / анализ целей.
- Помощь в создании совместных предприятий (JVs).
- Слияние компаний.

ECM-сделки на публичных рынках

Подготовка к IPO и помощь с:

- Привлечением pre-IPO раундов.
- Подготовкой маркетинговых материалов.
- Проведением переговоров.
- Структурированием размещения.

Research-портал. Собственный отдел исследований

- Покрытие 10+ отраслей.
- Бесплатный доступ к порталу с исследованиями для всех наших клиентов.

Реструктуризация (включая продажу части активов)

- Консультации по реструктуризации долга.
- Оптимизация портфеля активов.
- Привлечение сторонних инвесторов.

Широкая отраслевая специализация:

- Технологии, медиа, телекоммуникации.
- Потребительский сектор, розничная торговля и агросектор.
- Промышленное производство, инфраструктура и транспорт.
- Нефтегазовый сектор.
- Медицинские услуги и фармацевтика.
- Банки и финансовые организации.
- Банки и финансовые организации.

Команда и опыт

- С момента основания в 2008 г. Advance Capital стабильно входит в топ-5, а в последние годы занимает лидирующую позицию среди финансовых консультантов по сделкам M&A в России по версии Mergermarket.
- Команда Advance Capital закрыла более 100 сделок на сумму, превышающую US $5 млрд.
- Одна из крупнейших команд на рынке M&A в России, включая 6 партнеров и специалистов аналитического и управленческого состава с богатым опытом работы в ведущих международных инвестиционных банках, финансово-промышленных группах и индустриальных компаниях.
- Уникальный для российского рынка research-портал с доступом к ключевым рыночным данным и трендам в реальном времени, а также широкая сеть инвесторов, включая крупнейшие семейные офисы, позволяют выстраивать процесс эффективно, минимизируя риски и полностью удовлетворяя запросы клиентов.

Лидерство в рейтингах

- Топ-1 финансовый консультант по количеству M&A сделок в России по версии Mergermarket за 2022–2025 гг.
- 2025 — Лучший инвестиционный банк на венчурном рынке (Russia PE&VC Awards, PREQVECA).
- 2024 — Лучший инвестиционный банк для семейных офисов (WEALTH Navigator Awards).

- 2022, 2023 — Лучший инвестиционный банк на рынке M&A-tech (Russia M&A Awards, PREQVECA).
- 2022, 2023 — Лучший инвестиционный банк на венчурном рынке (Russia PE&VC Awards, PREQVECA).
- 2021 — Лучший локальный советник на российском рынке слияний и поглощений (Russia M&A Awards, PREQVECA).

Знаковые сделки в TMT

- Продажа 100% долей платформы для аналитики инфлюенс-маркетинга WhoIsBlogger.
- Продажа 49,99% долей производителя ЭЗС Е-ПРОМ фонду ВИМ Инвестиции.
- Продажа 100% долей сервиса онлайн-бронирования Академ-Онлайн Яндексу.
- Продажа 100% долей службы доставки Boxberry Яндексу.
- Продажа 60% долей программатик-платформы Hyper AdTech медиахолдингу РБК.
- Продажа контрольного пакета разработчика ВКС-решений VINTEO дочерней структуре МТС — МТС-Линк.
- Продажа медиапортала Pikabu.
- Продажа платформы бизнес-коммуникаций Jivo Сберу за 1,8 млрд рублей.
- Инвестиционный раунд для Borzo (ранее Dostavista) от нескольких крупных инвесторов (Mubadala, РФПИ и др.) на сумму $35 млн.
- Совместное предприятие между Maxima Telecom и Газпром-Медиа в области AdTech и Big Data с пониманием стратегических целей бизнеса клиентов.

ADVANCE CAPITAL



Евгений Антипов

партнер, управляющий директор



Дмитрий Касьяненко

партнер, управляющий директор



Артур Шубаев

партнер, исполнительный директор



Ярослав Кулешов

вице-президент



Вячеслав Поджаров

старший менеджер проектов



Владислав Ковтун

старший менеджер проектов

САЙТ ADVANCE CAPITAL →

ТЕЛЕГРАМ-КАНАЛ →

4

Приложение

Ограничение ответственности

Отказ от ответственности и использование данных исследования

1. Текст исследования не предназначен для потребителей

Материал не предназначен для потребителей, в том числе по смыслу Закона РФ «О защите прав потребителей»[46].

2. Текст исследования не является рекламой, консультацией или рекомендацией

Настоящее исследование подготовлено исключительно в информационных целях, является экспертно-аналитическим материалом, направленным на информирование о трендах на российском рынке Tech M&A в 2025 г., выявленных на основании методологии, указанной в Приложении 2 к настоящему исследованию.

Данное исследование не является рекламой, согласно пункту 3 части 2 статьи 2 Федерального закона «О рекламе»[47]. Ни само исследование, ни содержащиеся в нем текстовые, графические и иные материалы, сведения, утверждения, тезисы, статистические и аналитические данные, мнения, оценки, прогнозы не являются и не могут прямо или косвенно рассматриваться или истолковываться как юридическая, налоговая, инвестиционная, финансовая, бухгалтерская или иная профессиональная консультация или рекомендация, в том числе как рекомендация по ведению бизнеса. Никакие управленческие, финансовые, инвестиционные или иные решения не могут быть приняты на основе информации из данного исследования без предварительной консультации со специалистами, владеющими соответствующей экспертизой и квалификацией. Пользователи и читатели исследования не вправе полагаться на какие-либо данные и выводы исследования, в том числе при принятии или обосновании каких-либо управленческих или иных деловых решений.

3. Ограничение ответственности

Правообладатели, авторы, хедлайнеры (продюсеры), редакторы и участники исследования, авторы текста и комментариев, сотрудники, адвокаты и руководящий персонал компаний, фирм, адвокатских образований, инвестиционных банков, финансовых, юридических и иных консультантов, независимые эксперты, участвующие в исследовании и опросах, данные из которых приведены в исследовании, цитируемые эксперты, редакторы, а также любые лица, связанные с самим исследованием и формированием его выводов, будь то физические или юридические лица, не несут никакой ответственности (включая какие-либо убытки или ущерб) за какие-либо решения (и любые их последствия), действия или бездействие любых пользователей и читателей данного исследования, если таковые решения прямо или косвенно основаны на содержании данного исследования. Все такие решения принимаются пользователями и читателями данного исследования самостоятельно на свой собственный риск.

[46] Закон РФ от 07.02.1992 № 2300-1 «О защите прав потребителей».

[47] Федеральный закон от 13.03.2006 № 38-ФЗ «О рекламе».

Ничто в настоящем исследовании не является каким-либо заверением или любым другим юридическим обязательством авторов, правообладателей, экспертов, хедлайнеров и любых других лиц, упомянутых в исследовании, и ни при каких обстоятельствах не может быть истолковано в качестве таковых.

4. Цитаты и высказывания экспертов

Все цитаты, мнения, высказывания, оценочные суждения, выводы, а также любые фрагменты текста, представленные в данном исследовании, использованы с согласия их авторов, отражают исключительно их субъективное мнение по состоянию на дату составления данного исследования, действительны только на такую дату и могут в любое время быть изменены без какого-либо предупреждения или уведомления.

Такие цитаты, мнения, высказывания, оценочные суждения, выводы и тексты не могут рассматриваться в качестве позиции любых иных лиц (кроме их авторов), включая компании, фирмы, адвокатские образования, инвестиционные банки.

Авторы всех комментариев, использованных в тексте данного исследования, самостоятельно несут ответственность за их оригинальность и соблюдение ими прав третьих лиц в связи с подготовкой таких комментариев. Хедлайнеры и редакторы исследования не отвечают за оригинальность авторских комментариев и возможное нарушение ими прав третьих лиц.

Мнение правообладателей исследования может не совпадать с мнением авторов комментариев, приведенных в исследовании.

5. Актуальность и точность информации

Информация, представленная в данном исследовании, включая представленные прогнозы, тренды и тенденции, отражает исключительно личные оценочные мнения авторов, исходя из их субъективного понимания существа, специфики и точности соответствующих вопросов. Несмотря на стремление авторов и участников исследования предоставить актуальную информацию, не исключены ошибки, неточности и упущения. Авторы исследования не гарантируют полноту, надежность и точность информации, содержащейся в данном исследовании.

Правообладатели, хедлайнеры (продюсеры) и редакторы исследования не проводили какой-либо независимой проверки мнений, суждений, фактов, прогнозов и утверждений, содержащихся в авторских комментариях экспертов, и не несут никакой ответственности за их точность или полноту. Материал исследования, а также ссылки на упомянутые в нем законодательные акты и законопроекты, актуален по состоянию на 31.05.2026 г.

6. Отсутствие гарантии результатов

Какие-либо данные и прогнозы, представленные в настоящем исследовании, носят исключительно информационный характер и не являются гарантией будущих результатов или реализации прогнозируемых событий. Показатели, приведенные в отношении прошлых периодов, не обязательно свидетельствуют о достижении прогнозируемых результатов. Прогнозы, включенные в настоящее исследование, основаны исключительно на текущих предположениях по состоянию на дату составления исследования и могут меняться вследствие изменения различных факторов, влияющих на результат. Авторы исследования не обязаны уведомлять кого-либо о дальнейших изменениях выводов, прогнозов, факторов, трендов и тенденций, описанных в данном исследовании.

7. Ссылки на сторонние источники

Данное исследование может содержать ссылки на внешние информационно-аналитические источники и ресурсы. Авторы исследования не контролируют содержание таких сторонних источников, политик, режимов их конфиденциальности и практики их использования и не несут никакой ответственности за их соответ-

ствие требованиям законодательства, а также их возможное использование в рамках данного исследования.

8. Информация об авторском праве

Соправообладателем исследования являются Анастасия Нерчинская, DENUO, АЛРУД, VERBA LEGAL.

© 2026 Анастасия Нерчинская, АЛРУД, DENUO, VERBA LEGAL. Все права защищены.

Более подробная информация об авторском праве, а также правила цитирования каких-либо частей исследования приведены на страницах 4–5 исследования.

9. Персональные данные

Настоящее исследование содержит сведения о физических лицах, включая фамилию, имя, отчество, должность и место работы. Все персональные данные, представленные в данном исследовании, используются исключительно с согласия соответствующих субъектов персональных данных и в соответствии с требованиями законодательства Российской Федерации, включая Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Персональные данные используются исключительно в информационных целях, а также в целях подготовки, публикации данного исследования и его обсуждения в профессиональной среде и не подлежат распространению за рамками указанных целей.

10. Отсутствие в исследовании сравнения лиц, товаров и услуг

Фраза «лучшие практики», используемая в тексте настоящего исследования подразумевает, что такие практики являются лучшими исключительно по субъективному мнению комментаторов, экспертов и авторов соответствующего текста.

Хештеги #Лучшие_практики и #Мнение_лидеров_рынка, а также выражения «ведущие эксперты» и аналогичные им выражения используются исключительно для удобства навигации читателей по тексту исследования и не предполагают какого-либо сравнения каких-либо лиц, хозяйствующих субъектов и / или их товаров и услуг с иными лицами, хозяйствующими субъектами и / или их товарами и услугами или установления какого-либо превосходства каких-либо из таких лиц над другими лицами.

Комментарии под хештегами #Мнение_лидеров_рынка предоставлены представителями организаций, которые отмечены среди лидеров соответствующих рынков в одном или нескольких из следующих рейтингов: IFLR1000, Legal500, Chambers & Partners, Право-300, Коммерсант, Forbes, Mergers.ru, PREQVECA, Эксперт РА и / или Российская Газета.

11. Обратная связь

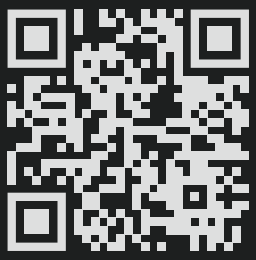
Мы приветствуем отзывы и комментарии пользователей и читателей исследования, однако не обязуемся учитывать их, в том числе в случае принятия нами решения об обновлении или пересмотре каких-либо частей исследования. Обратная связь может быть направлена корпоративным хедлайнерам исследования. Централизованный сбор обратной связи от читателей в рамках исследования не предусмотрен.



АНАСТАСИЯ НЕРЧИНСКАЯ

@SDELKIMNA →

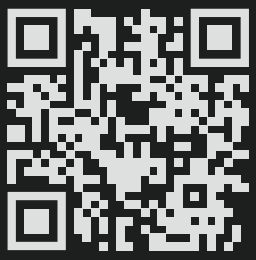
M&A I AI →



/ VERBA LEGAL

verba.legal →
+7 (495) 374-74-03

info@verba.legal
Москва, Гоголевский б-р, 11



АЛРУД

alrud →
+7 (495) 234-96-92
+7 (495) 926-16-48

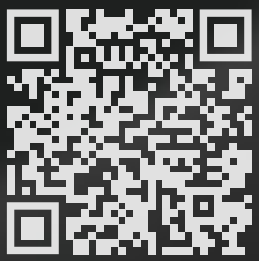
info@alrud.com
Москва, ул. Лесная, 7



Dénuo

denuo.legal →
+7 (495) 221-44-00

moscow@denuo.legal
Москва, Леонтьевский пер., 25



ADVANCE CAPITAL

advancecapital →
+7 (495) 161-67-00

info@advcap.ru
Москва, Пресненская наб., 12