

«ИИ-ЗООПАРК»: ПОЧЕМУ ЭНТУЗИАЗМ СОТРУДНИКОВ СТАЛ ОПЕРАЦИОННЫМ РИСКОМ

Теневой ИИ, абсорбционная способность и три модели организации функции

🕒 22 мин чтения • Цифровизация

Введение: проблема, которую уже проходили

Если коротко. Сотрудники уже используют ИИ в обход ИТ. Это не хаос, который нужно запретить, а способность, которую нужно построить: реестр инструментов, правила использования, контроль расходов и владелец функции. Кто этот владелец — главный управленческий выбор текста.

Тезис. Теневой ИИ-зоопарк — не проблема гигиены, а симптом: компания уже приняла ИИ, но ещё не построила способность его усваивать. Задача топ-менеджера — не запрет, а функция с мандатом на развитие, харнесом и интерфейсами с ИТ и ПРПС, которая превращает энтузиазм в измеримый операционный результат. Ниже — почему это операционный риск, как он выглядит в промышленности и какие структурные варианты есть у собственника и CEO.

ИИ-зоопарк — совокупность неучтённых и неуправляемых централизованно ИИ-инструментов и агентов, которые сотрудники используют в обход закупки и ИТ-ревью. Цифры и кейсы в статье приводятся по вторичным источникам; перед публикацией их следует сверить с первичными.

Промышленность всегда отставала от ИТ-отрасли в освоении новых инструментов. В этом нет ничего постыдного. ИТ-команды первыми прошли через облачную экспансию, DevOps, микросервисный хаос и болезненный переход к платформенной инженерии. Их

сегодняшние практики — не «модные эксперименты», а результат нескольких лет проб, ошибок и управленческих решений.

С ИИ происходит то же самое, только с одним отличием: скорость распространения инструментов внутри компании теперь выше, чем скорость, с которой ИТ успевает их замечать. И это уже не гипотеза, а измеренный факт.

Современная организация использует сотни приложений, и значительная их часть — теневой ИТ: инструменты, которые не проходили через закупку или ИТ-ревью. По оценкам поставщиков решений безопасности, большинство сотрудников хотя бы иногда используют неавторизованный ИИ, а формальная политика есть у меньшинства организаций. Точные проценты в таких обзорах зависят от выборки; для управленческого вывода важна не цифра, а устойчивое направление: теневой ИИ уже массовый.

Промышленность здесь не исключение. Отчёт Netskope Threat Labs (2025) показал, что в производственном секторе доля неразрешённых генеративных ИИ-инструментов хотя и снизилась с 83% в декабре 2024 года до 51% в сентябре 2025-го, но всё ещё остаётся сопоставимой с долей разрешённых инструментов — разрыв составляет менее 10 процентных пунктов.

Это не «проблема гигиены». Это три параллельных кризиса, которые накладываются друг на друга.

Кризис расходов. Токен-биллинг не ведёт себя как обычное облако: стоимость запроса зависит от длины контекста, выбранной модели, кэширования и количества шагов агента. Uber, по сообщениям, исчерпал годовой бюджет на ИИ за четыре месяца и был вынужден ввести лимиты после того, как внутренние лидерборды по использованию Claude Code превратились в ускоритель расходов. По данным FinOps Foundation, значительная часть организаций превысила первоначальные прогнозы по затратам на ИИ, а бюджеты растут быстрее, чем падает цена за токен. Парадокс в том, что цена за токен упала в разы, но счёт вырос, потому что никто не следит за тем, сколько токенов сжигается, на что и ради какого результата.

Кризис безопасности. IBM в отчёте Cost of a Data Breach 2025 обнаружила, что каждая пятая организация столкнулась с утечкой, связанной с теневым ИИ, и такие инциденты обходились в среднем на \$670 000 дороже среднего показателя. По данным Menlo Security, использование теневого генеративного ИИ за год выросло, а значительная часть пользователей теневых инструментов вводила конфиденциальные корпоративные данные в несанкционированные платформы. В промышленности это означает, что в промпт могут уйти параметры техпроцесса, данные о дефектах, фрагменты конструкторской документации. Анализ конфигураций агентных инструментов показывает, что значительная их часть позволяет агенту выполнять shell-команды и читать локальные

файлы, а их сочетание с сетевым доступом создаёт «токсичную трифекту», открывающую путь к эксфильтрации данных.

Кризис качества. McKinsey в обзоре The State of AI 2025 обнаружил: 88% организаций используют ИИ хотя бы в одной бизнес-функции, но только 39% респондентов говорят, что ИИ повлиял на их прибыль, и большинство из них сообщают о влиянии менее 5% на EBIT. По разным оценкам, около двух третей компаний остаются в фазе эксперимента или пилота. Gartner предупреждает, что более 40% агентных ИИ-проектов будут отменены к концу 2027 года из-за роста затрат, неясной бизнес-ценности и недостаточных механизмов контроля рисков. В промышленности цена ошибки агента — не испорченный слайд, а брак, простой или остановка линии.

Часть 1. Промышленность отстаёт — и это меняет природу проблемы

Отставание промышленности от ИТ-сектора в освоении ИИ — не оценочное суждение, а измеренный разрыв. По данным McKinsey (The State of AI 2025), использование ИИ-агентов в производстве остаётся ограниченным. Отраслевые исследования 2026 года показывают, что лишь небольшая доля производителей довела ИИ-пилоты до полного операционного развёртывания, а значительная часть промышленных компаний остаётся в «пилотном аду» — фазе, где пилоты запускаются, но не масштабируются, не окупаются и тихо умирают. Почему это важно для темы «зоопарка»? Потому что отставание промышленности создаёт иллюзию, что проблемы ИТ-отрасли сюда не дойдут. Логика «мы ещё не начали — значит, у нас нет зоопарка» опасна. Теневой ИИ в промышленности уже есть — цифры Netskope это подтверждают. Просто он менее видим, потому что промышленные компании реже имеют централизованные команды, которые его ищут.

Более того, у промышленности есть дополнительный фактор уязвимости: разрыв между ИТ-контуром и операционным контуром. ИИ-инструмент, который в ИТ-компаниях работает с кодом и документацией, в промышленной компании должен взаимодействовать с MES, SCADA, ERP и историческими данными оборудования.

Исследования в области промышленной безопасности прямо указывают на риск prompt injection через извлечённые материалы или выходы инструментов в среде OT, что может привести к поведению, противоречащему установленным политикам, и к ограниченной видимости из-за сбоев телеметрии. Один из участников обсуждения на Manufacturing LIVE сформулировал это так: «Вы за час собираете прототип, он потрясающий, все в восторге. А потом вы застреваете в пилотном аду на три недели, и он просто тихо умирает».

Часть 2. Как «зоопарк» выглядит вблизи: три промышленных сценария

Сценарий А: «Личные ассистенты». Сотрудники отдела снабжения используют ChatGPT на личных аккаунтах, чтобы писать письма поставщикам и переводить спецификации. ИТ об этом не знает. Данные уходят на внешние серверы, расходы не учитываются, а корпоративные стандарты конфиденциальности не применяются. По данным Menlo Security, значительная часть сотрудников использует бесплатные версии ИИ-инструментов через личные аккаунты, и многие из них вводят конфиденциальные данные. В производственном секторе Netskope фиксирует ту же динамику: доля неразрешённых инструментов снижается, но остаётся на уровне, сопоставимом с разрешёнными.

Сценарий Б: «Самодельные агенты». Технический директор попросил «автоматизировать отчётность». Энтузиаст из планово-экономического отдела собрал агента на MCP-сервере (Model Context Protocol — открытый протокол, через который агент подключается к внешним инструментам и источникам данных), который читает файлы из общей папки и формирует сводку. По данным отраслевых отчётов по безопасности, значительная часть MCP-серверов позволяет агенту выполнять shell-команды и читать локальные файлы, а их сочетание с сетевым доступом создаёт «токсичную трифекту» — сочетание доступа к приватным данным, возможности реагировать на недоверенный контент и канала отправки данных вовне. По данным отдельных обзоров конфигураций агентных инструментов, часть конфигураций устанавливает MCP-сервер без закреплённой версии, что создаёт риск supply-chain-атаки. Агент работает, отчёт формируется. Но если в промпт кто-то внедрит инструкцию, агент может сделать с файловой системой не то, что задумывал энтузиаст.

Сценарий В: «Золотая крыша на сарае». По сообщениям, Ford развернул систему ИИ-камер для контроля качества, полагая, что этого достаточно. Технология не смогла сравниться с суждением опытных инспекторов; компания, по тем же сообщениям, была вынуждена вернуть ветеранов-инженеров по качеству, чтобы те заново обучили системы и выступили внутренними аудиторами. Проблема была не в камерах. Проблема в том, что ИИ-слой положили поверх фрагментированных данных и неформализованного знания, которое никогда не было оцифровано. Ford — не исключение: по данным отраслевых опросов, устаревшая инфраструктура остаётся одним из главных барьеров для генеративного ИИ в производстве.

Часть 3. Почему энтузиазм и промпт-инжиниринг больше не работают

За три года дисциплина построения ИИ-решений прошла три сдвига. В 2023-м это был промпт-инжиниринг: искусство формулировать инструкцию. В 2024–2025-м — контекст-инжиниринг: искусство собирать правильное информационное окружение для модели. В 2026-м центр тяжести сместился к **харнес-инжинирингу** (от англ. harness — «упряжь», «обвязка»): проектированию runtime-обвязки вокруг модели — какие инструменты она может вызывать, как собирается контекст, где хранится память, как применяются политики, как отслеживаются запуски и обрабатываются сбои.

Это не академическая классификация. В работах по агентным системам харнес определяют как «программную и операционную конфигурацию, через которую большая языковая модель получает контекст, предлагает действия, использует инструменты, поддерживает состояние, возобновляет работу и производит эффекты вне самой модели». Ключевой вывод таких работ: агентная способность должна оцениваться на уровне пары «модель–харнес», а не модели самой по себе. Сильная модель может работать плохо в длительных задачах без стабильных интерфейсов, структурированной памяти, ограниченных разрешений и механизмов восстановления. Более скромная модель может работать надёжнее, когда харнес снижает неопределённость и ограничивает деструктивные действия.

Arize формулирует это ещё жёстче: харнес-инжиниринг — это «перенос полномочий, состояния, побочных эффектов и доказательств завершения в детерминированные runtime-контролы». Модель может выбирать, как решать задачу, но она не может расширять свои собственные разрешения, доверять устаревшему состоянию восстановления или объявлять об успехе без актуальных доказательств. Харнес определяет «конверт исполнения», за который модель не может выйти.

Для промышленной компании это означает простую вещь: надёжность ИИ-решения определяется не качеством промпта, а качеством ограничений. Промпт можно переписать, и поведение изменится. Харнес — это версионизируемая, аудируемая и воспроизводимая система, которая либо пропускает результат, либо блокирует его, независимо от того, насколько «удачно» сформулирован запрос.

Энтузиаст-сотрудник не может и не должен строить такой харнес. У него другая мотивация: быстро решить свою задачу. Это нормально. Но когда таких энтузиастов десятки, а харнеса нет ни у одного, компания получает зоопарк без ветеринара.

Часть 4. Почему это не про стандартизацию, а про абсорбционную способность

Ветеринар из предыдущей метафоры — это не конкретный человек и не отдел, а функция: набор ролей, правил и runtime-контролей, которые делают зоопарк управляемым. Дальше — зачем она нужна и кому её отдать.

Здесь самое время ответить на вопрос, который обычно остаётся за кадром: **зачем вообще нужна эта функция, если «зоопарк» — естественное проявление энтузиазма?** Сובлазн свести её миссию к «наведению порядка» велик. Но порядок — это побочный продукт. Настоящая цель глубже.

В теории управления есть концепция, которая описывает происходящее с пугающей точностью, — **абсорбционная способность** (absorptive capacity). Коэн и Левинталь определили её как «способность фирмы распознать ценность новой внешней информации, усвоить её и применить в коммерческих целях». Разница между компанией, которая *подвержена* ИИ, и компанией, которая *извлекает из него выгоду*, — это разница между экспозицией и абсорбцией. Сто сотрудников, каждый со своим ChatGPT, — это сто отдельных кривых обучения, которые никогда не пересекаются. Компания не учится. Она просто **потребляет** ИИ. Захра и Джордж (2002) уточнили модель, разделив потенциальную и реализованную абсорбционную способность: первая — умение найти и понять новое, вторая — умение превратить его в рутину и результат. «Зоопарк» — это высокая потенциальная и почти нулевая реализованная способность.

Именно поэтому «зоопарк» — идеальное алиби. Можно отчитаться: «мы используем ИИ в сорока сценариях», не имея ни одного измеримого эффекта на EBIT. Это **ИИ-театр** — ровно та же ловушка, что «цифровая трансформация», которая на деле оказалась оцифровкой бумажных форм в PDF. Формат сменился, процесс — нет. Ценность не возникла.

Чтобы увидеть, как это работает в исторической перспективе, достаточно вспомнить Excel. Его пытались запретить. ИТ-департаменты видели в нём угрозу: данные вне контура, макросы, неуправляемые вычисления. Запретить не удалось — потому что Excel давал людям агентность: возможность решить свою задачу без очереди в ИТ. Победила не бюрократия, а полезность.

Но вот что важно: компании, которые выиграли от Excel, не были теми, кто его запрещал, и не были теми, кто пускал всё на самотёк. Они построили **дисциплину работы с таблицами**: шаблоны, ревью моделей, стандарты финансового моделирования,

версионирование, разделение «расчётных» и «презентационных» листов. Они превратили хаотичный инструмент в управляемую способность.

И это не абстракция — у «зоопарка таблиц» есть измеренный ущерб. Исследования EuSpRIG фиксируют, что доля таблиц с ошибками в корпоративной практике оценивается в диапазоне от 78% до 90%. TransAlta потеряла около \$24 млн из-за ошибки copy-paste в Excel при подготовке заявок на энергетические контракты. Ошибка в таблице Рейнхарт–Рогоффа (2010) повлияла на дискуссию о политике жёсткой экономии в Европе. Один неверный символ в таблице привёл к тому, что на Олимпиаде в Лондоне-2012 были перепроданы 10 000 билетов на синхронное плавание.

Урок не в том, что «Excel плох». Урок в том, что **инструмент, который даёт агентность, неизбежно порождает риск — и зрелость компании измеряется не запретом, а способностью этот риск профессионализировать.**

Однако аналогия с Excel имеет предел, и этот предел принципиален. Excel детерминирован: один и тот же вход даёт один и тот же выход. Его можно открыть, посмотреть формулу, проследить зависимость. Blast-радиус ошибки — число в ячейке. ИИ-агент стохастичен и **обладает агентностью в другом смысле**: он не просто считает, он действует. Удаляет файл. Отправляет письмо. Выполняет shell-команду. Поведение агента не инспектируется «из коробки» — чтобы восстановить, что произошло и почему, нужен харнес: логи, трейсы, эвалы, механизмы отката. Нагрузка на управление у ИИ **выше**, чем у Excel, а не ниже.

Отсюда стратегический разворот. Большинство компаний рамкируют ИИ-управление как **защиту**: комплаенс, безопасность, «чтобы не утекло». Это защитная логика, и она проигрышна по определению — она не создаёт ничего, она только ограничивает. ИИ-инжиниринг — это **наступательная функция**. Она нужна не для того, чтобы «навести порядок», а чтобы превратить энтузиазм в **компаундищую способность**. Конкурентное преимущество не приходит из доступа к инструментам — доступ есть у всех (GPT, Claude, Gemini доступны каждому конкуренту). Оно приходит из **интеграции** инструментов в проприетарные процессы с проприетарными данными. А интеграция — это и есть работа ИИ-инженера. Без неё у компании есть доступ к ИИ, но нет преимущества.

Из этого следует и принцип дизайна функции: **не шлагбаум, а мощёная дорога**. Смысл не в том, чтобы запретить тропинки, а в том, чтобы санкционированный путь был объективно лучше теневого — удобнее, быстрее, безопаснее. Если одобренный инструмент хуже того, что сотрудник нашёл сам, он вернётся к теневому. Всегда. Поэтому метрика успеха ИИ-функции — не «сколько заявок мы отклонили», а **«скольким людям мы дали безопасно self-serve»**.

И честный контраргумент к самой себе: у этой функции есть встроенный риск — стать новой бюрократией, которая убьёт ту самую низовую энергию, из-за которой зоопарк возник. Excel был силен именно тем, что обходил ИТ. Решение — в мандате. Функция отвечает за **конверт исполнения** (что агенту можно, как логируется, как откатывается), но не за **выбор задачи**. Задача остаётся у бизнеса; функция даёт ему безопасный и дешёвый способ её решить. Это и есть различие между инжинирингом и контролем: инжиниринг проектирует возможности, контроль их запрещает.

Часть 5. Почему ИТ — не «владелец» этой функции, но и не «противник»

Это самый чувствительный вопрос для промышленной компании, где ИТ-директор часто является единственным человеком, который «хоть что-то понимает в технологиях». Ответ на него требует различения двух вещей: инфраструктуры и логики.

Разведём понятия, которые дальше встречаются рядом: ИИ-функция — организационная единица; ИИ-инжиниринг — деятельность; ИИ-инженер — роль; харнес — runtime-обязка вокруг модели.

В исследовании Harvard Business Review точно описан структурный разлом: «Команды ИИ и команды ИТ обычно объединяются под расплывчатым ярлыком “технологии”, но работают с фундаментально несовместимыми логиками. ИТ-команды оптимизируют контроль, стандартизацию и снижение риска. Команды ИИ требуют экспериментирования, гибкости и быстрого обучения». Это не различия в характерах или «культурная шероховатость». Это структурная несовместимость, встроенная в то, как каждая функция оценивается, финансируется и управляется.

HBR приводит конкретные точки конфликта. Данные: ИТ контролирует инфраструктуру, построенную для соответствия требованиям и аудируемости; командам ИИ нужен гибкий, экспериментальный доступ. Инфраструктурные решения: решение, которое ИТ корректно принимает с точки зрения риска, может сделать итерацию ИИ невозможной; решение, которое ускоряет обучение ИИ, может создать именно те пробелы в управлении, которые ИТ обязана предотвращать. Покрытие управления: ИИ производит новые формы данных, решений и результатов, для которых большинство систем управления ИТ не создавались. Но здесь есть важный нюанс, который часто упускают в дискуссии «отдать ИИ в ИТ или нет». ИТ-команды уже наработали решения, которые промышленность может адаптировать, не копируя организационную структуру. Харнес-инжиниринг, FinOps для ИИ, практики версионирования и аудита агентных конфигураций — всё это возникло именно в ИТ-среде, потому что ИТ столкнулась с этими проблемами раньше.

Промышленной компании не нужно изобретать эти практики заново. Ей нужно встроить их в свою операционную реальность — и для этого нужен человек или команда, которые говорят на языке и ИТ, и производства, но подчиняются логике развития, а не логике стабильности.

Если ИТ — не идеальный владелец, то кто? HBR фиксирует конфликт логик, а не готовую оргструктуру, поэтому ПРПС ниже — не вывод, а один из кандидатов. В промышленной компании есть функция, которая по своей природе ближе к логике развития, чем к логике стабильности, — подразделение развития производственных систем (ПРПС). Оно занимается не поддержанием текущего процесса, а его изменением: методологией, обучением, тиражированием улучшений. По духу ИИ-инженерия — сестра ПРПС. Обе функции работают через людей, обе по своей природе являются внутренним консалтингом, обе обречены на провал, если их KPI измеряются активностью, а не операционным результатом.

Но у этой сестры есть наследственная болезнь, которую нельзя игнорировать. Во многих компаниях ПРПС выродился в «службу 5С и отчётов»: активность есть, а измеримого влияния на себестоимость, простои или качество нет. Исследования показывают, что эффекты от проектов бережливого производства часто носят «виртуальный» характер, а корпоративный контроль правильности расчёта экономических эффектов не проводится. Одна из наиболее острых проблем — отсутствие компетентного заказчика, когда сотрудники ПРПС остаются наедине с проблемами, потому что на местах руководство не обладает необходимой компетенцией для постановки задач. Другая проблема — создание видимости изменений вместо выполнения реальной работы. ИИ-энтузиазм повторяет ту же траекторию, только быстрее и дороже. Поэтому простое помещение ИИ-функции в ПРПС без защиты от этой болезни воспроизведёт ту же ошибку. Структурное решение — это не выбор между ИТ и ПРПС, а выбор модели, которая сочетает мандат на развитие с иммунитетом к подмене результата активностью.

Часть 6. Варианты структурного решения: три модели и их условия

Модель А: «Симбиоз» (ИИ-функция как сектор внутри ПРПС). ПРПС даёт методологию работы с изменениями, доступ к «чемпионам» на местах и инфраструктуру доверия. ИИ-инженер привносит техническую экспертизу и харнес. Риск: ИИ-повестка растворяется в текучке Lean-проектов, а ИИ-инженер становится «человеком, который делает презентации про ChatGPT» для отчётов ПРПС. Условие успеха: прямой мандат от топ-менеджмента, отдельные KPI, защищённое время на исследование и пилоты.

Модель Б: «Параллельная структура» (выделенный ИИ-инженер или мини-СоЕ, подчинённый напрямую топ-менеджеру или техническому директору). Фокус исключительно на ИИ-зоопарке, экономике токенов и харнесе. ПРПС остаётся партнёром по внедрению изменений в цехах. Риск: дублирование функций обучения и работы с сопротивлением; изоляция от производственной реальности. Условие успеха: чёткие интерфейсы с ПРПС и с ИТ.

Модель В: «Гибрид» (Hub-and-Spoke для ИИ с опорой на ПРПС). Небольшой центральный «хаб» (ИИ-инженер плюс аналитик) отвечает за стандарты, харнес, экономику и отбор инструментов. «Спицами» становятся чемпионы в подразделениях, которых обучает и поддерживает ПРПС. ИТ отвечает за платформу, безопасность и администрирование. Риск: координационная сложность; необходимость чётких регламентов взаимодействия между тремя сторонами. Условие успеха: явное разделение — ИИ-хаб владеет «что и зачем», ПРПС владеет «как внедрить через людей», ИТ владеет «на чём и как безопасно».

МОДЕЛЬ	ВЛАДЕЛЕЦ	МАНДАТ	ИНТЕРФЕЙСЫ	ГЛАВНЫЙ РИСК	КОГ ВЫИ
А. Симбиоз	Руководитель ПРПС	Развитие через существующую методологию	ПРПС ↔ ИТ	Растворение в текучке; ИИ-инженер превращается в презентатора	Есть ПРП отде спел
Б. Параллельная структура	Топ-менеджер или технический директор	Только ИИ: экономика, харнес, зоопарк	Прямой выход на топ; партнёрство с ПРПС и ИТ	Изоляция от цехов; дублирование обучения	Уже крип тене быст расх
В. Гибрид (hub-and-spoke)	ИИ-хаб и владельцы в подразделениях	Хаб: стандарты и харнес; спицы: внедрение	Три стороны: хаб, ПРПС, ИТ	Координационная сложность; размытая ответственность	Неск плои бизн нужи маси

Эта модель не является теоретической конструкцией. Исследование организационных моделей для масштабирования ИИ показывает, что федеративная модель hub-and-spoke балансирует централизованный стратегический контроль и управление через AI Center of Excellence с децентрализованными, бизнес-ориентированными инновациями через встроенные кросс-функциональные команды. Для отраслей с высокой регуляторной сложностью и распределённой операционной структурой — а промышленность относится

именно к таким — эта модель позволяет масштабировать инновации быстрее, чем централизованная команда, и при этом не терять управляемость.

Часть 7. Бизнес-описание функции (неформально, но по существу)

Миссия. Обеспечить, чтобы каждый рубль, потраченный на ИИ, производил измеримый операционный результат, а каждый инструмент работал в управляемом контуре — с известными расходами, рисками и проверяемым качеством. Функция имеет право говорить «нет» инструментам, которые не проходят этот тест, и обязана предлагать альтернативу.

Что входит в зону ответственности. Ведение реестра всех ИИ-инструментов, включая теневые. Воронка заявок с оценкой по стратегической ценности, готовности данных и риска. Расчёт стоимости результата (не подписки) до запуска пилота. Создание и версионирование харнеса: правила, валидаторы, тесты, механизмы отката. Обучение — совместно с ПРПС, но с фокусом на ИИ-сценарии. Мониторинг расходов на токены и API с порогами и ранними предупреждениями.

Как выглядит успех (KPI, которые имеют смысл). Через 6 месяцев: все ИИ-инструменты учтены; как минимум один пилот завершён с измеримым эффектом на операционный показатель (простои, брак, скорость переналадки); расходы на ИИ видны в разрезе подразделений и задач. Через 12 месяцев: доля «управляемого» ИИ превышает долю «теневого»; как минимум два решения масштабированы за пределы пилотного подразделения; стоимость результата хотя бы для одного сценария снижена за счёт выбора более дешёвой модели или оптимизации контекста. **Что не является успехом:** количество пилотов, количество обученных, количество «внедрённых инструментов». Это метрики активности, которые уже похоронили репутацию многих ПРПС.

Организационный интерфейс. С ИТ: ИТ владеет инфраструктурой, закупками, администрированием и безопасностью; ИИ-инженер владеет выбором инструмента, экономикой и харнесом. Пересечение — через регулярный форум по архитектуре и чёткие SLA. С ПРПС: ПРПС владеет методологией изменений и обучением «мягким» навыкам; ИИ-инженер — техническим содержанием и стандартами. Совместные KPI — по операционному результату, а не по числу мероприятий.

Готовая рамка. Функции не нужно изобретать систему управления: NIST AI Risk Management Framework 1.0 (2023) задаёт цикл govern — map — measure — manage; ISO/IEC 42001:2023 — требования к системе менеджмента ИИ; EU AI Act (Regulation (EU) 2024/1689) — регуляторные обязанности для отдельных категорий систем. Для промышленной

компании это словарь, который привязывается к реестру инструментов и харнесу, а не заменяет их.

Заключение: выбор, который нужно сделать сейчас

«Зоопарк» ИИ-инструментов — это не признак того, что сотрудники делают что-то не так. Это симптом того, что компания уже приняла ИИ, но ещё не построила способность его **усваивать**. Excel прошёл этот путь за два десятилетия и оставил после себя целую профессию — финансовое моделирование — и целый пласт стандартов. ИИ пройдёт его быстрее, потому что цена ошибки выше, а окно конкурентного преимущества короче. Компания, которая построит ИИ-инжиниринг раньше, получит не «порядок», а **компаундищую способность** — и это стратегическая цель, а не гигиена.

У вас как у топ-менеджера есть три пути, и выбор между ними остаётся за вами — он не технический, а управленческий.

Первый путь: оставить всё как есть и надеяться, что зоопарк «самоорганизуется» в экосистему. Практика показывает, что он самоорганизуется в счёт, утечку и пилотный ад.

Второй путь: отдать ИИ-функцию в ИТ и получить стабильность, которая убьёт скорость экспериментов.

Третий путь: создать функцию с мандатом на развитие, но с иммунитетом к подмене результата активностью — и дать ей прямой доступ к операционным показателям, а не к отчётности о количестве обученных.

Функция инженера ИИ — не бюрократическая надстройка и не «ещё один ИТ-отдел». Это переводчик между скоростью экспериментов и требованиями промышленной надёжности. Без него зоопарк будет расти, а отдача — оставаться невидимой. С ним — у компании появляется шанс пройти путь, который ИТ-отрасль прошла за годы, за месяцы, и при этом не потерять ни данные, ни деньги, ни доверие производства.

Краткий чек-лист для читателя:

- ☐ Назначен ли владелец ИИ-функции с мандатом на развитие?
- ☐ Ведётся ли реестр всех ИИ-инструментов, включая теневые?
- ☐ Привязаны ли KPI функции к операционным показателям, а не к активности?
- ☐ Создан ли харнес с правилами, валидаторами и механизмами отката?
- ☐ Настроен ли мониторинг расходов на токены с порогами?

Источники

Cohen, W. M., Levinthal, D. A. Absorptive Capacity: A New Perspective on Learning and Innovation // Administrative Science Quarterly. — 1990. — Vol. 35, No. 1.

Zahra, S. A., George, G. Absorptive Capacity: A Review, Reconceptualization, and Extension // Academy of Management Review. — 2002. — Vol. 27, No. 2.

IBM. Cost of a Data Breach Report 2025.

McKinsey. The State of AI 2025.

Gartner. Over 40% of agentic AI projects will be canceled by end of 2027. — 2025.

Netskope Threat Labs. Cloud and Threat Report. — 2025.

Menlo Security. Cloud and Threat Report. — 2025.

FinOps Foundation. State of FinOps. — 2025.

EuSpRiG. Spreadsheet error research (arXiv:1401.7583).

NIST. AI Risk Management Framework 1.0. — 2023.

ISO/IEC 42001:2023. Information technology — Artificial intelligence — Management system. Regulation (EU) 2024/1689 (AI Act).

Harvard Business Review. Материал о разломе логик ИТ и ИИ. — 2026.

Читайте также

Цифровизация 1.0 (</articles/digital/cifrovizaciya-1-0/>). — почему единый источник правды — иллюзия и как читать стыки систем.

Цифровизация 2.0 (</articles/digital/cifrovizaciya-2-0/>). — гипотеза описания системы через объект, роли и события.

Неизбежное исполнение (</weapons/neizbezhnoe-ispolnenie/>). — 12 рычагов Медоуз: от слабых к сильным.

Геном завода (</genome/>). — типизированная библиотека процессов.

УПРАВЛЕНИЕ СПОСОБНОСТЬЮ

Серия о том, как компания подменяет способность её имитацией.

ЭКОНОМИКА

Throughput на час узкого места, TDABC и стоимость сложности — почему средняя себестоимость ошибается

 10 мин чтения

ЭКОНОМИКА

Почему инвестиции в качество управления не проходят инвестиционный комитет — и что с этим делать CEO и CFO

🕒 18 мин чтения

УПРАВЛЕНИЕ

Структурная ловушка, запас устойчивости и онтология понятий «развитие», «оптимизация», «антикризис»

🕒 20 мин чтения

ЦИФРОВИЗАЦИЯ

Атлас 22 стыков промышленного ИТ, три иллюзии и протокол диагностики

🕒 31 мин чтения

ЦИФРОВИЗАЦИЯ

Гипотеза описания системы: спецификации как правила связи, фронтير знания и режимы отказа

🕒 30 мин чтения

ЧАСТЫЕ ВОПРОСЫ

Что такое ИИ-зоопарк?

Это совокупность неучтённых и неуправляемых централизованно ИИ-инструментов и агентов, которые сотрудники используют в обход закупки и ИТ-ревью. Проблема не в самом энтузиазме, а в отсутствии контура, который превращает его в измеримый результат.

Почему теневой ИИ — операционный риск?

Он одновременно создаёт три кризиса: расходов (токен-биллинг и лимиты), безопасности (конфиденциальные данные уходят во внешние сервисы) и качества (пилоты не масштабируются и не дают эффекта на EBIT). В промышленности цена ошибки агента — брак, простой или остановка линии.

Кому отдать ИИ-функцию — ИТ или ПРПС?

Ответ не сводится к выбору между ИТ и ПРПС. В статье три модели: симбиоз внутри ПРПС, параллельная структура с прямым выходом на топ-менеджмент и гибрид hub-and-spoke. Выбор зависит от масштаба теневого ИИ, числа площадок и наличия сильного ПРПС.

С чего начать наведение порядка?

С реестра всех ИИ-инструментов, включая теневые, назначения владельца функции с мандатом на развитие и KPI по операционному результату, а не по числу пилотов и обученных. Затем — харнес с правилами, валидаторами, механизмами отката и мониторингом расходов на токены.

МАТЕРИАЛЫ ПО ТЕМЕ

Статья целиком и рабочие артефакты — для скачивания и печати.



Статья ««ИИ-зоопарк»: почему энтузиазм сотрудников стал операционным риском»

PDF • полный текст

СКАЧАТЬ

Разобрать вашу ситуацию

Опишите свой контур и ограничения — обсудим, где узкое место и что делать с экономикой, развитием и цифровым контуром.

НАПИСАТЬ В TELEGRAM