ПРАКТИЧЕСКИЙ ДЕЛОВОЙ ЖУРНАЛ

IT РЕВЬЮ

ОБЗОРЫ·КОММЕНТАРИИ·ПРАКТИКА

№2/2025

«сегодня ИИ – драйвер роста, и выигрывают те компании, которые уже его используют»

Вадим Медяник

BPA Technologies

Содержание

Подписные индексы:
По объединённому каталогу ГК РФ
Журнал издается при участии Историко-архивного института Российского государственного гуманитарного университета и Всероссийского научно-исследовательского института документоведения и архивного дела Росархива

Официальный адрес
TP@TOP-PERSONAL.RU
Гл. редактор
ИД «Управление персоналом»
Гончаров А. Н.

Электронное приложение к журналу «Управление персоналом»

Учредитель: ООО «Журнал «Управление персоналом».
Свидетельство о регистрации выдано Министерством РФ по делам печати, телерадиовещания и средств массовых коммуникаций ПИ № 77-15375 от 12 мая 2003 г.

Издатель: ООО «Топ-Персонал» с 2011 г.
Подписано в печать 30.03.2025.
Формат 60x90 1/8.

Главный редактор:
Александр Гончаров
Компьютерная вёрстка:
Наталия Риль
Корректоры:
Кочетков Павел, Сагун Ольга

Иллюстрации созданы ИИ:
Midjourney

Приглашаем директоров компаний поделиться опытом управления:
7447273@bk.ru

Важно быть честным:

модели искусственного интеллекта не всегда работают так, как это выглядит в презентациях

«С самого начала мы понимали: искусственный интеллект не должен быть игрушкой для экспериментов. Это инструмент, который помогает бизнесу экономить, ускоряться и принимать более точные управленческие решения».

ITРЕВЬЮ Искусственный интеллект и автоматизация – в чем вы увидели перспективу этих технологий?

Вадим Медяник
BPA Technologies

В начале наша работа была сосредоточена на разработке программных решений для бизнеса. Мы создавали продукты, которые помогали компаниям автоматизировать процессы, выстраивать аналитику и работать с данными. Это было естественным стартом: рынок в тот момент прежде всего искал надежные инструменты цифровизации.

Наш дальнейший поворот совпал с глобальными трендами. В последние 10 лет началось внедрение облачных AI-платформ от крупных игроков, появились десятки новых прикладных кейсов: от персонализации до интеллектуальной аналитики. Затем на рынок вышли генеративные модели, и интерес к искусственному интеллекту приобрел по-настоящему массовый характер: корпорации

начали интегрировать ИИ в ключевые продукты, а венчурные фонды инвестировали миллиарды в новые стартапы. Конкуренция между игроками усилилась одномоментно, появились специализированные нейросети для бизнеса и науки, а государства начали формировать первые регуляторные рамки. Фактически за эти года ИИ из экспериментальной технологии превратился в основной драйвер цифровой трансформации.

Поэтому на текущий момент у нас сложилась рабочая модель, которая позволяет закрывать большую часть запросов рынка в данном направлении. Это симбиоз трех направлений: инженерные решения («железо»), программное обеспечение и алгоритмы искусственного интеллекта. Такой подход позволяет строить комплексные продукты, которые не просто фиксируют и отображают данные, а понимают происходящее и помогают управлять процессами в реальном времени.

ITРЕВЬЮ Что такое искусственный интеллект для бизнеса сегодня?

— Нужно понимать, что сам термин «искусственный интеллект» во многом маркетинговая конструкция. Его действительно очень много видов, и это не единая «умная машина». Исторически первые основы были заложены математиками ещё в 50–60-х годах. Постепенно развивался математический аппарат, появлялись методы машинного обучения: сначала линейные приближения и простые предсказательные модели, затем деревья решений, алгоритмы оптимизации функций.

Позже пришло компьютерное зрение, когда машины научились различать образы на изображениях и видео, а затем популяризировалась обработка текста. То, что мы называем большими языковыми моделями, это относительно недавняя история. Массовый резонанс они вызвали только в начале 2020-х, когда на широкую публику вышли GPT-модели и вслед за ними десятки аналогов от других компаний. Сегодня на рынке множество игроков, которые активно развивают эти технологии.

Если говорить прикладным языком, искусственный интеллект сейчас — это экосистема моделей, каждая из которых заточена под свою задачу: обработка изображений и видео, генерация текста, синтез речи, анализ аудио, прогнозирование событий. Даже в привычном чат-боте вроде ChatGPT работает не одна система, а целый ансамбль: одна модель понимает речь, другая генерирует текст, третья может создать изображение или расшифровать аудио.

Для бизнеса ценность как раз в этом прикладном разнообразии, а также в том, что эти инструменты позволяют по-новому выстраивать управленческую архитектуру. Если раньше решения принимались на основе ограниченной статистики и отчетов «задним числом», то теперь компании получают данные и прогнозы в реальном времени. Это значит, что управленцы начинают действовать не постфактум, а проактивно.

Важно дополнить, что искусственный интеллект не заменяет человека, а дополняет его: помогает видеть то, что ускользает от внимания, прогнозировать события до того, как они наступили, и освобождать людей от рутины.

ITРЕВЬЮ Сегодня часто говорят об опасности: мол, вот ИИ уже превзошел человека в каких-то сферах. Достаточно вспомнить шахматы, когда Каспаров проиграл машине и это стало символом новой эпохи.
Можно ли провести параллель с бизнесом: действительно ли ИИ способен заменить человека, или он все же остается лишь инструментом?

— История с шахматами очень показательна. В 1997 году Гарри Каспаров проиграл суперкомпьютеру Deep Blue, и это стало символом того, что человек «уступил» искусственному интеллекту. Но важно понимать: шахматы — это узкая, чётко формализованная задача, где машина способна просчитывать миллионы вариантов вперёд. С таким перебором человек действительно не может конкурировать.

Позже многие говорили: хорошо, в шахматах машина сильнее, но есть игры вроде ГО — куда более сложные и стратегические, где машине никогда не обойти человека. В 2015 году AlphaGo впервые победила чемпиона Европы Фань Хуэя, а уже в марте 2016 года программа выиграла со счётом 4:1 у Ли Седоля, профессионала 9-го дана (высшего ранга), во время исторического матча, широко освещавшегося в прессе. Этот результат показал, что даже в областях, где интуиция и стратегия считались исключительно человеческой сильной стороной, ИИ способен находить неожиданные и победные решения.

В бизнесе ситуация похожая.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ БЛЕСТЯЩЕ СПРАВЛЯЕТСЯ ТАМ, ГДЕ ЕСТЬ ФОРМАЛЬНЫЕ ПРАВИЛА И НАКОПЛЕННЫЕ МАССИВЫ ДАННЫХ.

Он может анализировать, предсказывать, подсказывать лучшие решения. Но именно человек задаёт контекст, принимает риски и формирует стратегию, которая выходит за пределы любого алгоритма. Поэтому ценность рождается не в соревновании «кто умнее», а в тандеме: ИИ усиливает человека, а человек направляет ИИ.

ITРЕВЬЮ То есть для бизнеса это означает, что ИИ никогда не станет самостоятельным управленцем?

— Искусственный интеллект сегодня остаётся в первую очередь инструментом. Он может анализировать данные, предсказывать события, помогать в рутинных процессах. Но стратегические решения всё же принимает человек. При этом важно понимать: это ограничение связано не с принципиальной невозможностью, а с уровнем технологий на данный момент. Что будет через 3–5 лет — сказать сложно, и вполне вероятно, что роль ИИ в управлении изменится.

ITРЕВЬЮ Сегодня вокруг искусственного интеллекта очень много шума: одни компании рассказывают только об успехах, другие предупреждают о рисках. С какими ограничениями и проблемами бизнеса сталкиваются при внедрении ИИ-технологий?

— Тут важно быть честным: модели искусственного интеллекта не всегда работают так, как это выглядит в презентациях. Многие компании, когда рассказывают об успехах, упускают из виду ошибки. А ошибки там есть всегда. Если говорить про генерацию текста, то такие модели стохастичны и если долго переспрашивать одну и ту же задачу, можно получить совершенно разные ответы: сначала «да, всё будет хорошо», потом «нет, всё плохо». Это нормально для алгоритма, но бизнесу важно понимать, что такие системы не дают стабильного результата «раз и навсегда».

Кроме того, многие из этих моделей обучены так, что склонны «галлюцинировать», то есть выдавать выдуманную информацию с видом абсолютной уверенности. В маркетинге или при генерации текстов карточек товаров это не критично. Но если мы говорим про промышленность или управление персоналом, цена ошибки может быть очень высокой. Поэтому всегда нужно четко разделять, где можно полагаться на модель, а где требуется контроль человека. И еще один момент: сейчас инвесторы и рынок находятся в состоянии эйфории. Буквально недавно Сэм Альтман, глава OpenAI, открыто говорил, что рынок языковых моделей похож на пузырь, и по его оценке он даже больше, чем пузырь доткомов начала 2000-х. То есть часть решений перегрета, и далеко не все стартапы выживут. Но это естественный процесс: рынок должен пройти этап «перегрева», после чего останутся компании, которые реально создают ценность, а не просто используют модное словосочетание «Artificial intelligence» в презентации.

Поэтому я бы сказал так:

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ СЕГОДНЯ — ЭТО МОЩНЫЙ ИНСТРУМЕНТ В УМЕЛЫХ РУКАХ.

Он может сэкономить миллионы, но может и навредить, если применить его без понимания ограничений. Самое главное, правильно выбирать задачи, в которых такая технология должна использоваться.

ITРЕВЬЮ А если перейти от теории к практике: какие конкретные задачи ваши проекты на базе искусственного интеллекта уже решают для бизнеса и промышленности?

— Мы действительно работаем в разных направлениях, и задачи сильно отличаются в зависимости от отрасли.

В ритейле, например, наши системы компьютерного зрения помогают менеджменту видеть, как реально живет магазин: определять пустоты на полках и несоответствия ценников, понимать поведение покупателей и фиксировать попытки воровства,

контролировать работу сотрудников. Это информация в режиме реального времени, которая позволяет принимать управленческие решения и экономить деньги компании.

В рамках промышленных кейсов можно говорить о контроле качества продукции. На фабриках мы ставим камеры, которые с помощью искусственного интеллекта выявляют брак на разных этапах производства. Причем система различает десятки видов дефектов и сразу фиксирует их в учетных системах. Это позволяет моментально отсекать бракованные изделия и не пускать их дальше по конвейеру.

Есть и более креативные применения. Например, генерация описаний карточек товаров для маркетплейсов. У крупного продавца каждую неделю появляются сотни новых товаров. Если это вручную писать, то понадобятся десятки копирайтеров. Сегодня же достаточно передать системе название и пару параметров, и текст готов в нужном формате. Это экономия времени и снижение рутины предприятия.

Другой кейс, уже из научной сферы. К нам недавно обращался институт по изучению одного из древних языков с идеей перевода старинных текстов. Проблема в том, что качественных переводов очень мало, а самих сочинений насчитывается тысячи. Это огромный пласт культуры, который остается недоступным исследователям и широкой аудитории. И вот именно здесь языковые модели реально помогают открывать новое знание. Они могут обрабатывать тексты, переводить их на русский язык, формировать первые черновики, которые потом редактируют ученые. Это работа, которая руками заняла бы десятилетия, а с ИИ становится возможной уже сейчас.

Есть и направление, связанное с людьми. По паттернам поведения, например, как сотрудник пишет письма, как общается с коллегами, как меняется его рабочая активность, можно предсказывать его стресс или выгорание. Система может предупредить менеджера и помочь человеку раньше, чем ситуация станет критичной. Это очень актуально в условиях, когда компании возвращают людей из удаленки в офис или наоборот меняют формат работы.

ITРЕВЬЮ Если говорить о промышленности: может ли искусственный интеллект не просто фиксировать инциденты, а предсказывать аварии и пожары ещё до того, как они произойдут?

— Да, такие системы уже существуют и показывают высокую эффективность. Здесь преимущество искусственного интеллекта очевидно: он анализирует данные без перерывов и усталости. У человека со временем «замыливается глаз», снижается внимание, появляются

ошибки, особенно после долгих смен. Машина же одинаково точно работает и в первый, и в пятидесятый час.

Что касается пожаров: мы делаем решения, которые распознают задымление или очаги возгорания в открытых пространствах, на улице, в ангарах, где обычные датчики дыма плохо работают или их физически невозможно поставить. Но в ряде промышленных кейсов речь идет не только о распознавании дыма или огня, а именно о прогнозировании. Система анализирует технологический процесс и фиксирует предвестники аварии. Например, заносятся данные о похожих случаях на зарубежных заводах, учитываются сроки эксплуатации станков и оборудования, и алгоритм может подсказать: через 30 часов определенном узле высока вероятность поломки или через 15 дней потребуется техническое обслуживание системы.

Здесь работают специализированные модели, не такие как в чат-ботах. Они принимают данные сразу с десятков датчиков, обучены на реальных исторических событиях и умеют находить закономерности: какие сигналы предшествуют поломке или аварии. На основании этого система выдает рекомендации касательно корректировки режима эксплуатации или, например, проведения внепланового техобслуживания.

Фактически это переход от реагирования к прогнозированию. И в промышленности такие решения особенно ценны, потому что они позволяют не просто минимизировать последствия, а предотвратить ЧП ещё до его возникновения.

ITРЕВЬЮ Как вы видите роль искусственного интеллекта в производственных компаниях, где уже внедрена глубокая автоматизация? Например, на металлургических заводах или фабриках: сможет ли ИИ дать что-то принципиально новое, или здесь достаточно роботов и конвейеров?

— На мой взгляд, искусственный интеллект в промышленности является логичным продолжением автоматизации. Роботы и конвейеры выполняют операции, но им все равно нужен «мозг», который будет анализировать данные и подсказывать управленцам, как действовать дальше. Именно эту роль и берет на себя ИИ.

У нас есть несколько показательных кейсов. Первый — деревообрабатывающее предприятие. Там мы внедрили систему контроля качества, которая в режиме реального времени выявляет до 50 видов брака и производит подсчет объема проделанной работы. Камеры фиксируют дефект, система автоматически передает данные в учетную

систему. Это фактически цифровой аналог знаменитой практики Toyota, где рабочий мог остановить конвейер при обнаружении ошибки, только здесь все работает мгновенно и без человеческого фактора усталости. Но конечное решение все равно за человеком, который управляет процессом.

Другой пример приведу в такой небанальной отрасли, как переработка отходов. Там идет стык автоматизации и ИИ. Конвейерная лента распределяет сырье по фракциям, а алгоритмы компьютерного зрения определяют материалы: пластик, бумагу, металл, отделяют несортируемые отходы. Самую тяжелую и монотонную работу теперь берет на себя система, а человеку остается роль оператора, который контролирует работу, вмешивается в нестандартных ситуациях и отвечает за общее качество процесса.

Экономический эффект здесь огромный: меньше брака, меньше простоев оборудования, меньше издержек.

ITРЕВЬЮ Если бы у вас было безлимитное финансирование, какой проект в области искусственного интеллекта вы бы сделали в первую очередь?

— Безлимитное финансирование, любой срок, любые люди... Ну это прямо идеальные условия, которых в жизни не бывает даже по отдельности. Обычно всё наоборот: времени меньше, задачи амбициознее, а людей всегда не хватает. Но тем интереснее пофантазировать.

Если говорить честно, я бы сделал полноценную систему «Умный город». Причем не набор отдельных решений, а именно цельную платформу, которая объединяет транспорт, безопасность и инфраструктуру.

Представьте: беспилотные автомобили не только видят дорогу своими датчиками, но и обмениваются информацией между собой и с городом. Машина знает не только то, что происходит вокруг нее, но и что случилось за пару километров впереди: авария, пробка или ремонт.

К этому подключается «умная» инфраструктура: камеры и светофоры управляются автоматически, система сама оптимизирует потоки, включает зеленый там, где нужно разгрузить дорогу, или подсвечивает пешехода ночью для безопасного перехода.

Частично отдельные элементы таких технологий уже тестируются, но цельного решения пока нет. А именно оно сделало бы город по-настоящему безопасным, удобным и эффективным. Мечтать-то не запрещено, и, по моему опыту, иногда именно такие мечты становятся реальными проектами.

ITРЕВЬЮ А если посмотреть с другой стороны: когда технологии становятся такими мощными, неизбежно встает вопрос об ограничениях. Использование искусственного интеллекта все чаще поднимает вопросы этики. Считаете ли вы, что компаниям нужны новые правила и стандарты в этой сфере?

— Да, и это абсолютно неизбежно. Чем шире ИИ проникает в жизнь, тем больше рисков, как, например, некорректные решения и манипуляция данными. Поэтому нужны понятные правила игры: где технологии допустимы, а где их применение может навредить человеку. Важно, чтобы компании не относились к этике как к формальности, а действительно проектировали системы с прицелом на безопасность и прозрачность. Кстати, в этом году мы стали подписантами Кодекса этики по ИИ. Потому что доверие пользователей — это самая ценная валюта для любых ИИ-решений.

ITРЕВЬЮ А что вас лично вдохновляет в работе с искусственным интеллектом?

— Для меня такие новые технологии — это про возможность делать невозможное. Когда видишь, как алгоритм помогает находить дефекты, которые человек не заметил бы, или переводит тексты, которые десятилетиями лежали мертвым грузом, понимаешь, что технологии реально открывают новое знание. А еще вдохновляет сама динамика. В этой сфере невозможно заскучать: каждый год появляются инструменты, которые меняют рынок и твой взгляд на профессию

*Вадим Медяник,
технический директор компании BPA Technologies

Редактор Л. Веселова · Корректор О. Сагун · Дизайн Н. Риль
Эксклюзивно для ITРЕВЬЮ

Информационная безопасность крупных компаний и аутсорсеры как причина утечек

Когда компания передаёт часть функций подрядчикам, она фактически открывает внутренний периметр для внешних игроков. Даже если отношения оформлены контрактом и регламентированы политиками безопасности, аутсорс остаётся одной из самых уязвимых точек. Данные важнее денег.

Александр Вайс,
WEB3Bureau

Представьте, еще сто лет назад грабители в шляпах и сомбреро с винчестерами останавливали поезда, а условные Бонни и Клайд грабили банки, вскрывали сейфы и уходили с мешками наличных. Сегодня, чтобы получить доступ к деньгам, оружие больше не нужно. Достаточно украсть доступ — и ты уже внутри банка или внутри всей компании.

Всем давно понятно, что деньги — это больше не купюры. Это данные. Управление транзакциями, клиентские базы, конфиденциальные документы, пароли, приватные ключи. Доступ к этим данным ровняется контролю над бизнесом. Особенно в FinTech и DeFi, где одна скомпрометированная строка в коде или незащищённый API может стоить десятки миллионов долларов.

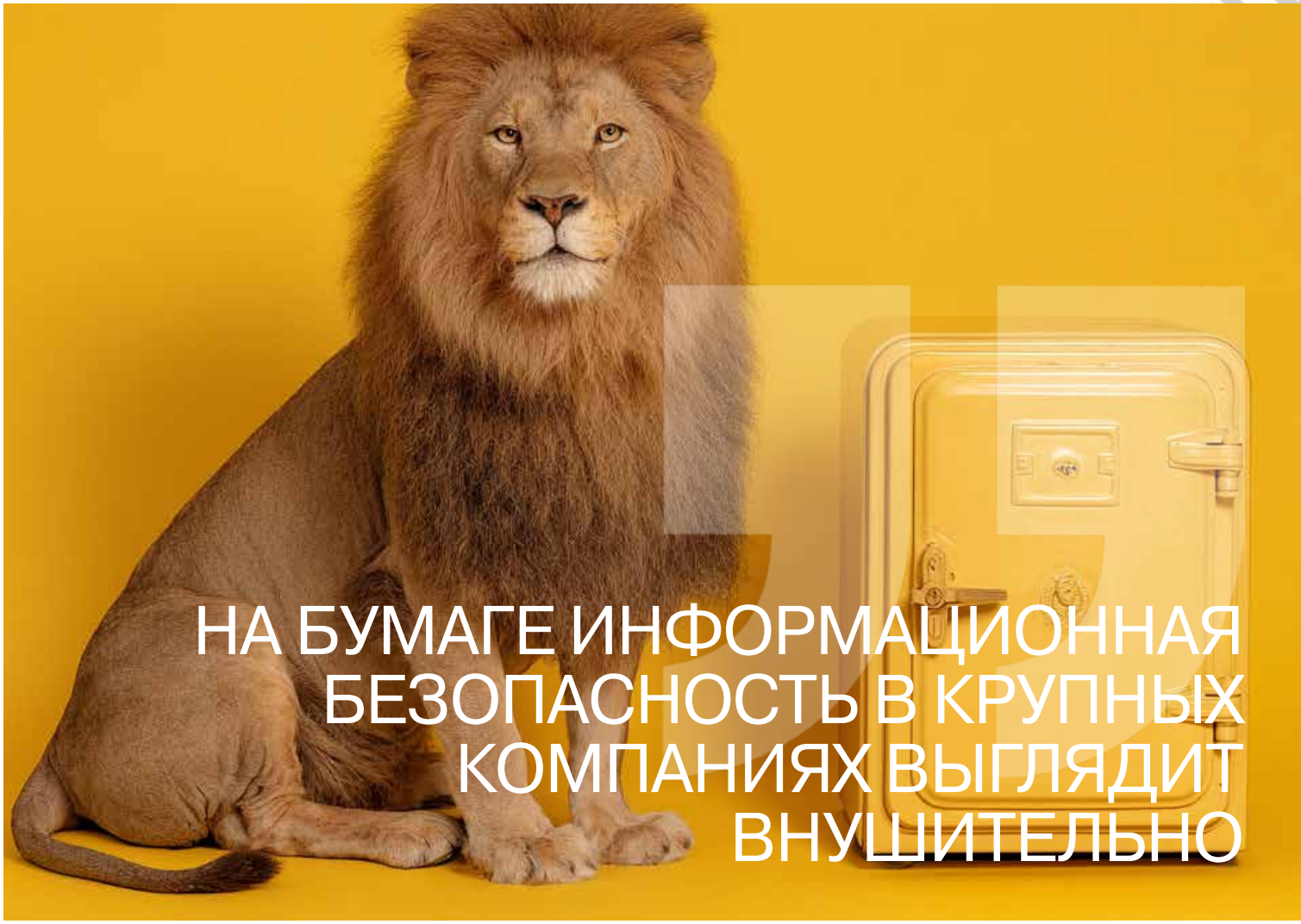
Но при этом парадокс: чем больше компания, тем больше людей вовлечены в процессы, тем чаще она

делегирует задачи вовне — и тем больше у неё уязвимостей. Безопасность рушится не от продвинутых атак, а от обычной логистики доступа. И всё чаще — это не внутренние сотрудники, а подрядчики, фрилансеры, агентства.

Аутсорс стал нормой — это удобная и быстрая оптимизация работы. Но с ним пришёл и новый класс угроз. Когда внешний подрядчик получает доступ в вашу систему, он автоматически становится частью периметра. И если вы не контролируете, как он работает, вы теряете контроль над своей безопасностью.

В этой статье я разберу, как и почему аутсорсеры становятся причиной утечек, на что не обращают внимания крупные компании, и как выстроить процессы так, чтобы внешние люди не становились внутренней угрозой.

Как работает корпоративная информационная безопасность в реальности.



Есть политики безопасности, утверждённые руководством, регулярно обновляемые процедуры реагирования на инциденты, внутренние регламенты, аудит и целый арсенал технических средств — от DLP-систем до SIEM-платформ. Работает Центр мониторинга безопасности (SOC), ведутся логи, проводятся тренинги по кибер-гигиене, а ежегодные аудиты подтверждают соответствие стандартам ISO/IEC 27001, PCI DSS, GDPR и другим.

На практике формализм и бюрократия часто подменяют реальную эффективность. Документы пишутся «под аудит», SOC перегружен событиями и сигналами тревоги, которые никто не успевает анализировать, а тренинги превращаются в обязательную «галочку» в системе корпоративного обучения.

В результате — все формальности соблюдены, а риск утечки данных остаётся критически высоким. Руководство уверено, что защита работает, потому что отчёты — в порядке, но отчётность не равно безопасность.

Аутсорс — удобный, но рискованный ресурс

Под аутсорсерами сегодня понимается широкий круг внешних специалистов и компаний, которым передаются функции, ранее исполнявшиеся внутри организации. Формально они не являются частью компании, но часто имеют доступ к её внутренним данным, системам и даже ключевым процессам.

Главные причины — экономия, гибкость и нехватка собственных специалистов. Аутсорсинг позволяет быстро закрыть задачи, не тратя ресурсы на найм, обучение и удержание персонала.

Аутсорс как канал утечки данных

Когда компания передаёт часть функций подрядчикам, она фактически открывает внутренний периметр для внешних игроков. Даже если отношения оформлены контрактом и регламентированы политиками безопасности, аутсорс остаётся одной из самых уязвимых точек. Почему?

Удалённый доступ

Почти все аутсорсеры работают удалённо: через VPN, терминальные сессии, облачные панели администрирования. Это значит, что защита физического периметра компании

перестаёт играть роль — злоумышленник может попасть внутрь, скомпрометировав удалённого подрядчика.

Удалённый доступ часто предоставляется не по принципу минимальных привилегий, а «для удобства» — полный доступ к средам разработки, базам данных, административным интерфейсам. Такие уровни доступа дают огромные возможности как для легитимной работы, так и для утечки.

Общие ключи, VPN, SSH

Типичная практика — одна учётная запись или один ключ доступа на всю команду подрядчика. При увольнении одного специалиста пароль или ключ часто остаются без изменений. В случае компрометации отследить виновника практически невозможно.

Даже если используются более безопасные методы, такие как SSH с ключами, компании редко реализуют полноценную систему управления этими ключами: ротация, логирование, аудит — всё это делается нерегулярно или только «на бумаге».

Человеческий фактор: низкая мотивация, текучка, субподряд

Аутсорсеры, особенно на нижнем уровне, редко вовлечены в культуру безопасности компании-заказчика. Они не чувствуют ответственности за данные, не понимают последствий и часто работают «по шаблону». У них может не быть достаточной квалификации.

Дополнительно усиливают риски:

Текучка кадров в аутсорсинговых компаниях — человек сегодня работает, завтра уходит, но доступы остаются.

Низкая мотивация — подрядчики заинтересованы в скорости выполнения задачи, а не в защите данных.

Субподряд — если задача передаётся третьим сторонам, это создаёт слепую зону для основного заказчика: кто на самом деле работает с его данными, уже неясно.

Реальные инциденты: утечки данных через подрядчиков и сопутствующий ущерб

Практика показывает, что именно через внешние подрядные структуры злоумышленники

нередко получают доступ к критически важной информации. Вот реальные кейсы таких утечек.

Revolut: компрометация через человеческий фактор

В сентябре 2022 года финтех-компания Revolut сообщила об инциденте безопасности. Были скомпрометированы персональные данные более 50 000 клиентов. По официальной информации, утечка произошла в результате атаки с использованием социальной инженерии, направленной на одного из сотрудников или подрядчиков из клиентской поддержке.

В результате несанкционированного доступа были раскрыты имена пользователей, электронные адреса, номера телефонов, адреса проживания и в отдельных случаях — сведения о платёжных картах. Revolut подчеркнула, что инцидент не повлиял на финансовые операции, однако последствия потребовали вовлечения регуляторов и информационного уведомления затронутых клиентов.

SolarWinds: масштабная атака через цепочку поставок

Один из наиболее значимых инцидентов последнего десятилетия произошёл в 2020 году, когда в процессе обновления ПО SolarWinds Orion был внедрён вредоносный код. Согласно отчётам, компрометация произошла на этапе CI/CD — сборочного пайплайна, обслуживаемого внешними техническими партнёрами.

Злоумышленники получили доступ к внутренним сетям более 18 000 компаний и правительственных организаций, включая агентства США. Уязвимость оставалась незамеченной в течение нескольких месяцев, что указывает на системные проблемы в контроле за безопасностью сторонних подрядчиков и поставщиков программного обеспечения.

Tesla: утечка интеллектуальной собственности бывшим сотрудником

В июне 2025 года компания Tesla подала судебный иск против своего бывшего инженера, обвинив его в неправомерном использовании конфиденциальных материалов, касающихся проекта гуманоидного робота Optimus.

После ухода из компании специалист основал собственный стартап и, по заявлению Tesla, использовал внутренние документы и технические наработки, к которым имел доступ во время работы.

Хотя в данном случае речь идёт не о классическом аутсорсере, инцидент иллюстрирует общую проблему — передача чувствительной информации сотрудникам, в том числе временным или внешним, без надлежащего контроля за дальнейшим использованием этих данных. Это особенно актуально при работе с подрядчиками, где механизмов мониторинга и юридической ответственности зачастую ещё меньше.

Каждый из этих кейсов повлёк за собой значительные финансовые и репутационные потери. Даже тщательно отобранные подрядчики остаются фактором риска. Отсутствие прозрачного контроля и полной интеграции их в систему корпоративной безопасности делает возможными подобные инциденты.

Как выстроить безопасную работу с аутсорсерами?

Передача функций внешним подрядчикам — неизбежная реальность для большинства современных компаний. Но она не должна означать потерю контроля или компромисс в вопросах информационной безопасности. Ниже перечислил ключевые принципы, которые позволяют сделать работу с аутсорсом управляемой и безопасной.

1. Контракт как инструмент защиты

Контракт — не просто формальность, а первое звено в системе безопасности. Он должен чётко регулировать:

Уровни доступа: какие системы доступны подрядчику, с какими правами.

Обязанности по защите данных: соответствие требованиям ISO 27001, GDPR, локальным законам.

Ответственность за инциденты: кто и в каком объёме несёт последствия при утечке данных или сбое.

Политику субподряда: запрет или согласование привлечения третьих лиц.

Права на аудит: возможность проверок со стороны заказчика, в том числе без предварительного уведомления.

Чем конкретнее прописаны условия и последствия — тем меньше правовой и операционный риск.

2. Zero Trust как основа архитектуры

Принцип Zero Trust («не доверяй, проверяй») должен применяться ко всем внешним командам — независимо от их репутации или длительности сотрудничества.

Базовые принципы:

Подрядчик — это не доверенное лицо — каждый доступ, каждое действие должно быть проверяемым и обоснованным.

Проверка личности и устройства — обязательна. Используйте многофакторную аутентификацию, контроль устройств, геолокацию и другие механизмы.

Сегментация доступа: ни один подрядчик не должен иметь сквозной доступ к инфраструктуре. Всё должно быть разбито по ролям, зонам и средам.

Zero Trust — это не технология, а подход. Его можно реализовать постепенно, даже в существующих системах.

3. Минимизация доступа: только то, что нужно, и только тогда, когда нужно

Наиболее распространённая ошибка — дать подрядчику «максимум, чтобы он не мешал». Это удобно, но опасно.

Что нужно внедрить:

Доступ по времени (Just-In-Time Access): доступ предоставляется только на период выполнения конкретной задачи и автоматически отзывается после завершения.

Доступ по задаче: права ограничиваются необходимыми ресурсами — например, только к dev-среде, только с чтением и тд.

Регулярный пересмотр доступа: ежемесячная ревизия прав пользователей, включая подрядчиков. Ушёл человек — права аннулируются немедленно.

Используйте инструменты управления привилегиями (PAM-системы), особенно если подрядчики получают административные доступы.

4. Контроль, обучение, аудит

Без регулярного контроля никакая модель доступа не будет эффективной. Что необходимо включить в процессы:

Аудит активности: логирование всех действий подрядчиков в чувствительных системах, с возможностью быстрого анализа.

Мониторинг аномалий: использование SIEM и UEBA-систем для выявления нетипичных действий со стороны внешних пользователей.

Обучение подрядчиков: они должны проходить базовое обучение по политике безопасности заказчика, включая правила работы с конфиденциальной информацией.

Периодические проверки и опросы: включая внешние и внутренние аудиты, а также оценку уровня зрелости ИБ у подрядчика.

Безопасность — это процессы и культура, в которой каждый участник, включая внешние команды, понимает свою зону ответственности.

Надёжный аутсорс возможен только при системном подходе. Чёткие контракты, архитектура Zero Trust, минимальные права доступа и постоянный контроль — ключевые элементы, без которых невозможно обеспечить реальную безопасность.

*Александр Вайс,
Серийный FinTech and DeFi предприниматель, разработчик и аналитик WEB3Bureau

Редактор Л. Веселова · Корректор О. Сагун · Дизайн Н. Риль
Эксклюзивно для IT РЕВЬЮ

Информационная безопасность крупных компаний: аутсорсинг как источник уязвимостей

Современные компании, стремящиеся к оптимизации процессов и сокращению издержек, всё чаще прибегают к аутсорсингу и интеграционным решениям, по оценке Дмитрия Ляхова, директора по информационной безопасности Сервиса «Грузовичкоф». Такой подход позволяет сосредоточиться на ключевых бизнес-функциях, делегируя специализированные задачи подрядчикам. Однако в последние годы стало очевидно, что привлечение сторонних исполнителей не всегда сопровождается повышением безопасности — напротив, нередко создаёт новые риски и уязвимости, которые становятся причиной утечек данных.

Дмитрий Ляхов,
«Грузовичкоф»

В эпоху цифровизации корпоративные инфраструктуры включают не только внутренние ИТ-системы, но и внешние сервисы: облачные платформы, аутсорсинговые службы, интеграторов, подрядчиков. При этом обеспечение безопасности требует комплексного подхода — как технического, так и организационного. Важно выстраивать прозрачную систему взаимодействия со всеми участниками цепочки, включая координацию, контроль и аудит всех участников процесса.

Выбор надёжного внешнего партнёра становится критически важным элементом защиты данных. Компании должны оценивать не только технологические возможности поставщика, но и

его зрелость в вопросах ИБ (информационной безопасности): наличие регламентов, способность к быстрому реагированию, готовность к совместному управлению рисками. Надежный партнер не только соблюдает высокие стандарты защиты данных, но и активно участвует в совместной работе по выявлению и минимизации рисков. Эффективное взаимодействие предполагает регулярные аудиты, обмен информацией об угрозах, выработку общих стандартов безопасности.

В конечном итоге, успешная защита зависит от уровня доверия и сотрудничества между всеми сторонами, вовлеченными в корпоративную экосистему.

Существует распространённое заблуждение, что информационная безопасность касается только внутренней инфраструктуры компании. Для обеспечения надежной защиты данных применяют целый эшелон классов защиты (EDR, SIEM, NGFW и прочих средств защиты информации). По мере усложнения проектов компании все больше полагаются на аутсорсинг IT-сервисов. Эти связи создают не просто внешние зависимости, но и потенциальные угрозы для безопасности. Каждая новая интеграция может стать точкой атаки, увеличивая риск утечек данных и других инцидентов.

Сложность ситуации заключается в том, что зачастую не всегда есть возможность контролировать внутренние процессы своих партнеров. Например, сторонняя компания может внедрять решение для защиты данных, но не позаботиться о его своевременном обновлении, отсутствии уязвимостей в своей инфраструктуре. Это явление «сапожника без сапог», когда даже самые опытные специалисты порой игнорируют свои собственные рекомендации. Кроме того, на аутсорсинге могут работать с данными, не соблюдая необходимые стандарты и внутренние регламенты компании, с которой они сотрудничают.

Существуют и более прямые примеры нарушения безопасности. Фиксировали у себя случаи, когда сторонние аутсорсинговые компании осуществляли перебор паролей, при этом утверждая, что проблем с безопасностью не наблюдается. Также выявлялись инциденты, когда одна и та же учетная запись использовалась несколькими сотрудниками подрядчика без предварительного согласования, что в итоге приводило к внутренним расследованиям и необходимости пересмотра политик доступа.

Совсем недавно, в ходе исследований одной из компаний в области информационной безопасности, было выявлено, что количество атак через поставщиков выросло втрое только за этот год. Особенно это актуально для компаний с георасределённой инфраструктурой и высокой степенью цифровой интеграции, где влияние внешних факторов на безопасность особенно велико.

На фоне таких рисков усиливается внимание к договорной ответственности подрядчиков. На практике это означает, что в договорах с внешними партнерами прописываются детализированные пункты о компенсации ущерба в случае утечек данных. Также обязательным становится установление сумм компенсаций за утечку, при этом с точки зрения законодательства ответственность всегда возлагается на оператора, а в договорных отношениях с аутсорсинговыми компаниями фиксируется только порядок и размер возможных компенсаций.

Одной из эффективных мер защиты является внедрение решений управления привилегированным доступом (PAM). Эти решения позволяют контролировать доступ к чувствительным данным и критическим системам, ограничивая права пользователей, имеющих доступ к важной информации, и предотвращая несанкционированное использование или утечку данных. Однако полагаться исключительно на один класс решений недостаточно для полноценной защиты от инцидентов. Обеспечение безопасности требует комплексного и системного подхода — сочетания технологий, организационных регламентов и зрелой культуры ИБ.

Аутсорсинг и интеграции с внешними партнерами в современных бизнес-процессах — это неотъемлемая часть эффективной работы компании. Однако эта практика несет в себе значительные риски утечек данных, если к ней не подходить с должной осторожностью. Важно помнить, что безопасность бизнеса не ограничивается только своей инфраструктурой, и обеспечение ее требует тщательной работы с внешними поставщиками.

Информационная безопасность — не изолированная функция, а постоянный процесс, требующий внимания к деталям, ответственности всех участников и стратегического видения. Только стратегический подход к управлению безопасностью и сотрудничество с надежными поставщиками, основанное на прозрачных обязательствах и четкой ответственности, помогут компаниям снизить риски и сохранить защиту на всех уровнях взаимодействия.

*Дмитрий Ляхов, директор по информационной безопасности Сервис «Грузовичкоф»

Редактор Л. Веселова · Корректор О. Сагун · Дизайн Н. Риль
Эксклюзивно для IT РЕВЬЮ

Ключ к снижению угроз — комплексный подход

Информационная безопасность крупных компаний и аутсорсеры как причина утечек

В эпоху цифровой трансформации информационная безопасность становится одним из ключевых факторов устойчивости и конкурентоспособности крупного бизнеса. Утечки данных способны не только нанести прямой финансовый ущерб, но и разрушить доверие контрагентов, партнеров, инвесторов. Особое внимание в последние годы уделяется роли интеграторов и аутсорсеров — сторонних компаний и специалистов, которым передаются функции по обслуживанию ИТ-инфраструктуры, разработке программного обеспечения, поддержке бизнес-процессов. Именно взаимодействие с интеграторами и аутсорсерами все чаще становится причиной крупных инцидентов, связанных с утечкой конфиденциальной информации, взломах и шифровании.

Дмитрий Беляев,
ООО АБТ

Рост числа и сложности кибератак

В 2025 году отмечается устойчивый рост числа киберинцидентов, а также увеличение их сложности. Крупные компании сталкиваются с атаками, использующими современные технологии, включая искусственный интеллект и LLM, социальную инженерию, сложные вредоносные программы и эксплойты уязвимостей. При этом дефицит квалифицированных специалистов по ИБ вынуждает бизнес все чаще прибегать к услугам внешних подрядчиков и аутсорсеров, и нередки случаи, когда один человек работает на 3 и более компании сразу.

Основные угрозы:

- Смишинг/Фишинг и социальная инженерия (обман сотрудников с целью получения доступа к системам);
- Вредоносное ПО и эксплойты;
- DDoS-атаки на инфраструктуру;
- Утечки данных через внутренние и внешние каналы;
- Нарушения политик безопасности и человеческий фактор.

Почему компании выбирают аутсорсинг

- Оптимизация затрат на ИТ и безопасность;
- Доступ к экспертным знаниям и современным технологиям;
- Возможность сосредоточиться на основном бизнесе;
- Гибкость в масштабировании ресурсов.

Основные риски аутсорсинга

Риск Описание

Потеря контроля Сложность мониторинга действий интегратора/аутсорсера, особенно если он работает удаленно

Недостаточная квалификация подрядчика Не все интеграторы/аутсорсеры обладают необходимым уровнем экспертизы и зрелыми процессами ИБ

Нарушения конфиденциальности Риск передачи или утраты коммерческой тайны, персональных данных, критической информации

Технические уязвимости Использование устаревших или неправильно настроенных решений, отсутствие регулярных обновлений

Внутренние угрозы Недобросовестные сотрудники интегратора/аутсорсера могут сознательно или случайно стать источником утечки

Юридические и регуляторные риски Несоблюдение требований законодательства по защите данных, особенно при трансграничной передаче информации

Аутсорсеры как причина утечек данных

Механизмы возникновения утечек через аутсорсеров:

1. Умышленные действия сотрудников подрядчика

- Кража данных с целью продажи конкурентам или злоумышленникам;
- Саботаж и внедрение вредоносного ПО.

2. Ошибки и небрежность

- Неправильная настройка серверов, открытые порты, слабые пароли;
- Использование незащищенных каналов передачи данных.

3. Недостаточный контроль доступа

- Избыточные права сотрудников интегратора/аутсорсера к корпоративным ресурсам;
- Отсутствие мониторинга действий подрядчиков и своевременной блокировки доступов.

4. Нарушения политик безопасности

- Отсутствие или формальный характер соглашений о конфиденциальности (NDA);
- Игнорирование требований по шифрованию, резервному копированию, журналированию действий.

5. Технические уязвимости

- Использование устаревших или несертифицированных решений, отсутствие патчей и обновлений;

- Неавтоматизированное управление доступом и учетными записями.

Примеры реальных инцидентов

Сноуден и подрядчик АНБ: Один из самых известных случаев, когда сотрудник подрядной компании получил доступ к секретной информации и организовал ее утечку, что привело к глобальному скандалу и пересмотру политики работы с аутсорсерами в государственных и частных структурах. В России и мире фиксируются регулярные инциденты, когда подрядчики, обслуживающие ИТ-инфраструктуру или разрабатывающие ПО, становятся источником компрометации данных из-за ошибок, халатности или злого умысла.

Причины уязвимости крупных компаний

Человеческий фактор:

- Сотрудники аутсорсера могут не иметь достаточного уровня подготовки по вопросам ИБ;
- Высокая текучесть кадров у подрядчиков затрудняет контроль и обучение персонала;
- Недостаточная мотивация к соблюдению стандартов безопасности.

Организационные проблемы:

- Отсутствие четких регламентов взаимодействия с подрядчиками;
- Недостаточная детализация SLA (Service Level Agreement) по вопросам ИБ;
- Формальный подход к заключению NDA и других юридических документов.

Технические аспекты:

- Использование подрядчиками собственных ИТ-решений и инфраструктуры, несовместимых с политиками безопасности заказчика;
- Нехватка инструментов для мониторинга и аудита действий подрядчиков в режиме реального времени.

Каналы и типы утечек данных:

- Электронная почта (пересылка файлов вне защищенных каналов):
- Съемные носители (флешки, внешние диски);
- Облачные сервисы и мессенджеры;
- Печать и копирование документов;
- Неавторизованный доступ к корпоративным системам;
- Удаленный доступ через VPN без 2FA, RDP и другие протоколы.

Как минимизировать риски утечек через аутсорсеров

Юридические меры:

- Подробное прописывание ответственности за утечку в договорах и NDA;
- Введение штрафных санкций и компенсаций за инциденты;
- Обязательное заключение соглашений о неразглашении с каждым сотрудником подрядчика.

Организационные меры:

- Проведение аудита подрядчиков перед началом сотрудничества;
- Регулярное обучение и инструктаж сотрудников аутсорсера по вопросам ИБ;
- Внедрение многоуровневого контроля доступа и принципа минимальных привилегий;
- Мониторинг и аудит всех действий подрядчика в корпоративной инфраструктуре.

Технические меры:

Использование DLP-систем для предотвращения утечек данных;

- Шифрование каналов передачи информации;
- Регулярное обновление программного обеспечения и патчей;
- Внедрение SIEM и SOC для мониторинга событий безопасности в реальном времени.

Примеры лучших практик:

- Крупные компании внедряют многоуровневую систему контроля подрядчиков, включая обязательную сертификацию по стандартам ИБ, регулярные проверки и аудит;
- Использование специализированных решений для мониторинга активности подрядчиков и автоматического выявления аномалий в поведении.

Перспективы развития и новые вызовы:

- Внедрение искусственного интеллекта и автоматизации в процессы мониторинга подрядчиков позволяет быстрее выявлять подозрительную активность и реагировать на инциденты;
- Рост числа облачных сервисов и удаленных рабочих мест увеличивает сложность контроля над аутсорсерами и требует новых подходов к защите данных;
- Усиление регуляторных требований (например, по персональным данным) вынуждает компании более тщательно выбирать подрядчиков и инвестировать в совместные меры по обеспечению безопасности.

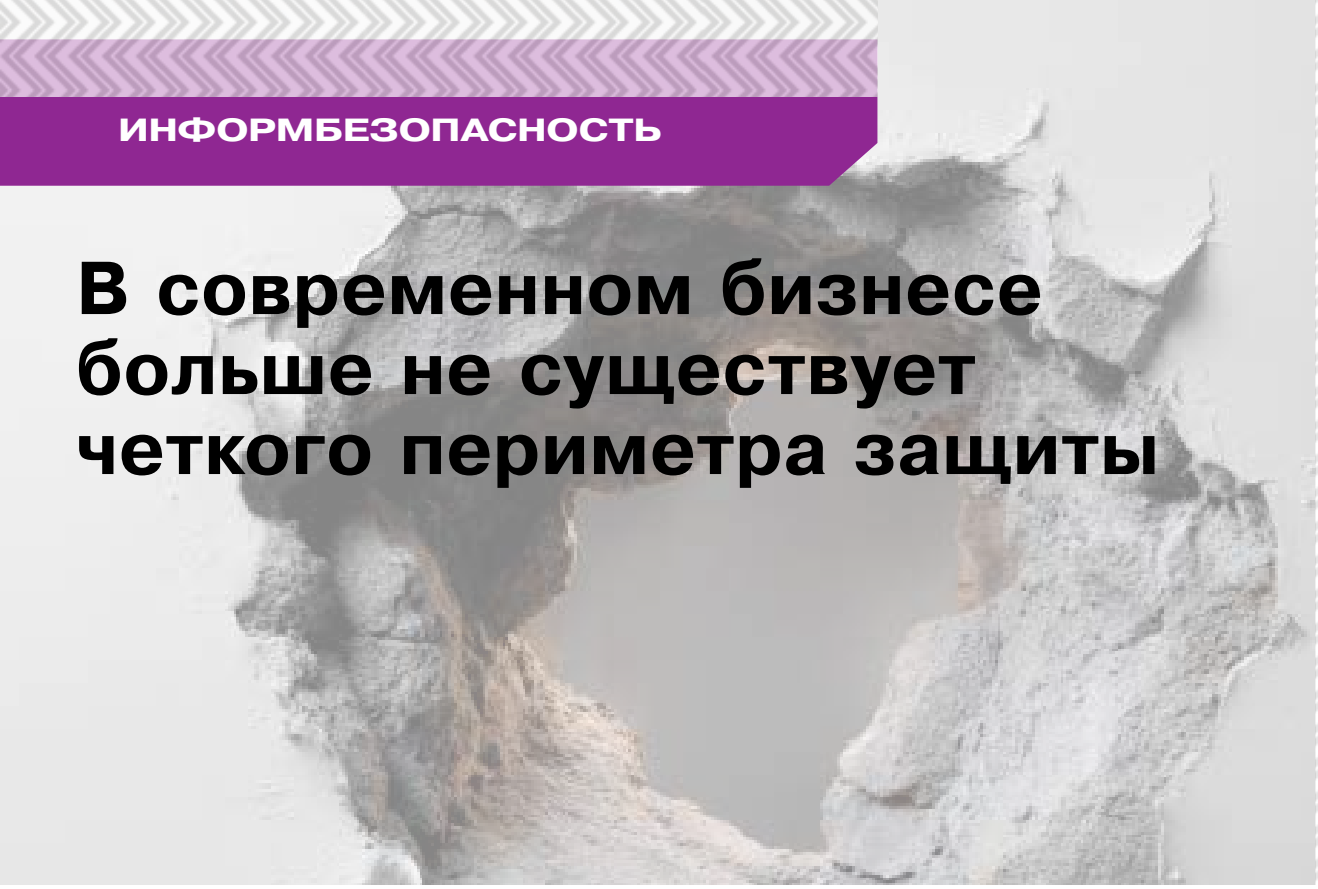
Аутсорсинг остается эффективным инструментом оптимизации бизнес-процессов и повышения конкурентоспособности крупных компаний, однако всё еще многие компании его остерегаются. Важно понимать, что передача доступа к корпоративным данным внешним подрядчикам неизбежно повышает риски утечек информации. Ключ к снижению угроз — комплексный подход: сочетание юридических, организационных и технических мер, а также постоянный мониторинг и обучение всех участников процесса. Только так можно сохранить доверие клиентов, партнеров и обеспечить безопасное развитие бизнеса в условиях растущих киберугроз и векторов атак.

*Дмитрий Беляев, Директор по кибербезопасности ООО АБТ

Редактор Л. Веселова · Корректор О. Сагун · Дизайн Н. Риль

Эксклюзивно для IT РЕВЬЮ

В современном бизнесе больше не существует четкого периметра защиты



В эпоху цифровой трансформации информационная безопасность становится одним из ключевых факторов устойчивости и конкурентоспособности крупного бизнеса. Утечки данных способны не только нанести прямой финансовый ущерб, но и разрушить доверие контрагентов, партнеров, инвесторов. Особое внимание в последние годы уделяется роли интеграторов и аутсорсеров — сторонних компаний и специалистов, которым передаются функции по обслуживанию ИТ-инфраструктуры, разработке программного обеспечения, поддержке бизнес-процессов. Именно взаимодействие с интеграторами и аутсорсерами все чаще становится причиной крупных инцидентов, связанных с утечкой конфиденциальной информации, взломах и шифровании.

Представьте, что

ВЫ ПОТРАТИЛИ МИЛЛИОНЫ НА СТРОИТЕЛЬСТВО НЕПРИСТУПНОЙ ЦИФРОВОЙ КРЕПОСТИ. У ВАС ВЫСОКИЕ СТЕНЫ - ФАЙРВОЛЛЫ ПОСЛЕДНЕГО ПОКОЛЕНИЯ. У ВАС БДИТЕЛЬНАЯ СТРАЖА - СОБСТВЕННЫЙ ШТАТ СПЕЦИАЛИСТОВ ПО БЕЗОПАСНОСТИ. У ВАС СЛОЖНЫЕ ЗАМКИ - МНОГОФАКТОРНАЯ АУТЕНТИФИКАЦИЯ. А ПОТОМ ВЫ НАНИМАЕТЕ САДОВНИКА ДЛЯ УХОДА ЗА ГАЗОНОМ, ОТДАЕТЕ ЕМУ КЛЮЧ ОТ БОКОВОЙ КАЛИТКИ И НЕ СПРАШИВАЕТЕ, КУДА ОН ЕГО КЛАДЕТ НА НОЧЬ. АБСУРД? ИМЕННО ТАК СЕГОДНЯ ВЫГЛЯДИТ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ 9 ИЗ 10 КРУПНЫХ КОМПАНИЙ, АКТИВНО ПРИВЛЕКАЮЩИХ ВНЕШНИХ ИСПОЛНИТЕЛЕЙ.

Меня зовут Петр Сухоруких, и моя работа - спасать репутацию компаний после катастроф. Я могу сказать вам с полной уверенностью:

САМЫЕ РАЗРУШИТЕЛЬНЫЕ УТЕЧКИ ДАННЫХ, КОТОРЫЕ МНЕ ПРИХОДИЛОСЬ РАЗГРЕБАТЬ, ПРОИСХОДИЛИ НЕ ИЗ-ЗА ГЕНИАЛЬНЫХ АТАК НА ЯДРО КОРПОРАТИВНОЙ СЕТИ. ОНИ ПРОСАЧИВАЛИСЬ ЧЕРЕЗ ТУ САМУЮ КАЛИТКУ - ЧЕРЕЗ НОУТБУК ДИЗАЙНЕРА-ФРИЛАНСЕРА, ЧЕРЕЗ ПЛОХО НАСТРОЕННЫЙ СЕРВЕР МАРКЕТИНГОВОГО АГЕНТСТВА, ЧЕРЕЗ СОТРУДНИКА ВНЕШНЕГО КОЛЛ-ЦЕНТРА.

В современном бизнесе больше не существует четкого периметра защиты. Он простирается до каждого партнера, которому вы доверяете свои данные. И главный парадокс заключается в том, что, передавая задачи внешним исполнителям ради эффективности, вы импортируете риски, которыми зачастую совершенно не управляете. Вы можете делегировать разработку, маркетинг или бухгалтерию, но вы никогда, ни при каких обстоятельствах, не сможете делегировать и ответственность.

Точки входа: где именно протекает ваш корабль?

Давайте прекратим говорить абстрактно и посмотрим на конкретные, до боли знакомые примеры уязвимостей, которые создает привлечение сторонних команд.

«Креативное» маркетинговое агентство. Вы передаете им свою базу клиентов для email-рассылки - святая святых вашего бизнеса. А у них в штате три веселых дизайнера и один аккаунт-менеджер. Никакого выделенного специалиста по ИБ, пароли от CRM хранятся в общем файле в облаке, а сотрудники регулярно работают из кафе с публичным Wi-Fi. Они - идеальная точка входа для злоумышленника.

Надежная юридическая фирма на подряде. Маленькая, уважаемая компания, которая ведет ваши самые сложные дела. Вы отправляете им по почте сканы договоров, коммерческие тайны, M&A-документацию. А у них вся инфраструктура - это три ноутбука и обычный роутер из магазина электроники, который не обновлялся с момента покупки.

Команда разработчиков на аутстаффе. Вы наняли талантливых программистов, которые пишут вам код нового продукта. Но они работают из разных стран, с личных компьютеров, на которых кроме вашей интеллектуальной собственности установлены торрент-клиенты, компьютерные игры и десятки других приложений сомнительного происхождения. Системный администратор-фрилансер. Вы наняли его для настройки облачного хранилища. Он сделал свою работу и ушел. Но он допустил одну маленькую ошибку в конфигурации, из-за которой ваша база данных оказалась в публичном доступе. А вы узнали об этом из новостей, когда информация уже утекла.

Цепь доверия: как взять подрядчиков под контроль

Перестать работать со сторонними командами - не вариант. Научиться управлять их рисками - единственный путь. Это не требует огромных вложений, это требует системного управленческого подхода.

Шаг 1. Due diligence «под микроскопом». Прежде чем подписать договор, вы должны провести аудит безопасности партнера так же тщательно, как финансовый аудит. Запросите их внутренние регламенты. Узнайте, как они обучают персонал, как управляют доступами, как реагируют на инциденты. Если в ответ вы слышите молчание или невнятное мычание - это красный флаг. Отсутствие формализованных политик в этой сфере - гарантия будущих проблем.

Шаг 2. Контракт как ваше главное оружие. Ваш стандартный договор на оказание услуг здесь не подойдет. В соглашении с любым подрядчиком, имеющим доступ к вашим данным, должен быть отдельный, детально проработанный раздел, посвященный защите информации.

- что считается конфиденциальными сведениями.
- как они должны храниться и передаваться (шифрование обязательно).
- кто несет финансовую ответственность в случае утечки по их вине.
- каков порядок действий при инциденте (они обязаны уведомить вас в течение нескольких часов, а не недель).

- ваше право на проведение инспекции их инфраструктуры.

Шаг 3. Принцип минимальных привилегий. Никогда не давайте партнерам доступ «с запасом» или «для удобства». Маркетологам нужна только выгрузка email-адресов? Дайте им только эти сведения, без телефонов и истории покупок. Разработчику нужен доступ к тестовой среде? Он не должен иметь допуска к продуктивной базе данных. Каждый избыточный доступ - лишняя потенциальная дыра в вашей обороне.

Шаг 4. Постоянный мониторинг и «учебные тревоги». Не заблуждайтесь: подписанный договор не снижает риски, он лишь дает вам право ими управлять. И с этого момента это ваша прямая обязанность. Включайте подрядчиков в периметр ваших внешних тестов на проникновение (пентестов). Устраивайте внезапные проверки. Требуйте ежеквартальные отчеты о принимаемых мерах безопасности. Спросите их прямо: «Что вы будете делать, если ваш сотрудник потеряет ноутбук с данными наших клиентов? Покажите мне ваш план реагирования».

Не ваша вина, но ваша репутация

Позвольте мне объяснить, что произойдет, когда утечка случится по вине вашего партнера. Заголовки в СМИ будут кричать название вашей компании, а не их. Иск от клиентов будет подан против вас. Штраф от регулятора придет на ваш юридический адрес.

В глазах всего мира нет никакой разницы, на чьем именно сервере произошел инцидент. Есть только один факт: вы, как оператор данных, не смогли обеспечить их сохранность. Вы несете полную репутационную, финансовую и юридическую ответственность. Поэтому главный вопрос, который должен задать себе сегодня каждый руководитель - это не «Насколько хорошо защищена наша компания?». Правильный вопрос звучит так: «Насколько надежно самое слабое звено в нашей цепи поставок данных?». И ответ на него определяет реальный уровень вашей безопасности.

*Петр Сухоруких, предприниматель, эксперт по антикризисному PR, основатель международного агентства цифровой репутации «Невидимка»

Редактор Л. Веселова · Корректор О. Сагун · Дизайн Н. Риль

Эксклюзивно для ITРЕВЬЮ

УДЕРЖАНИЕ IT СПЕЦИАЛИСТОВ

Как удержать IT-таланты в компании, если высокая зарплата уже не гарантирует лояльности?

Высокой заработной платой больше не удержишь?

Да, одной высокой зарплаты сегодня, действительно, недостаточно. Она по-прежнему остаётся важным фактором при выборе компании, но уже не играет ключевой роли в удержании. Особенно в IT, где сильные специалисты работают не за «ставку», а за смысл, развитие и комфорт.

Что действительно работает:

1. Ощущение влияния и смысла. Люди хотят видеть, как их работа отражается на продукте и бизнесе. Это не просто про «я сделал задачу», а про осознание своей ценности. Когда специалист видит, что его решения внедряются, и понимает, зачем он это делает, мотивация возрастает в разы.

2. Открытая коммуникация и участие в жизни команды. IT-специалист остаётся в команде, когда его слышат. Когда он может проявлять инициативу, получать честную обратную связь и видеть, что его мнение действительно важно. Руководители, которые выстраивают открытый и уважительный диалог, дольше удерживают сильных специалистов — не только благодаря премиям и бонусам, а прежде всего, за счёт человеческого отношения. Там, где есть доверие и смысл, команда не разваливается при первом же оффере с рынка.

3. Сильный и реальный пакет бенефитов. Не просто “ДМС и печеньки”, а то, что реально ценится:

- ДМС, включающий психолога, массаж, стоматологию и другое
- Финансирование курсов, сертификаций, профильных конференций - разные способы повышения квалификации

- Компенсация спортзала, wellness-программ

- Возможность работать удалённо или гибридно

4. Создание комфортного рабочего пространства. Уют и функциональность физического офиса важны даже для гибридных форматов. Это не излишество, а вложение в производительность и комфорт. Уютная кухня, тёплое освещение, пуфики, удобные кресла, тихие зоны и пространства для отдыха — всё это имеет значение. Особенно, когда есть возможность отвлечься: поиграть в приставку, перекинуться партией в настольный теннис или просто выдохнуть. Такой перерыв помогает переключиться и с новыми силами вернуться к задачам.

Но настоящая забота — не только про интерьер. В некоторых компаниях для сотрудников даже организуют частные детские сады. Это не просто «корпоративная забота», а искреннее внимание к людям, их комфорту и жизненному балансу.

5. Корпоративная жизнь, в которую хочется включаться. Люди остаются в компаниях, где им интересно. Где с коллегами не просто “по работе”, а по-настоящему общаешься. Где есть доверие, ценности, общее видение. Особенно это важно на удалёнке — хорошо налаженное онлайн-взаимодействие и регулярные встречи оффлайн реально работают.

6. Гибкость и доверие. Строгий контроль и микроменеджмент демотивируют. IT-специалисты ценят, когда компания доверяет им, когда есть гибкий график, свобода в выборе инструментов, подходов и даже формата работы. Главное — результат, а не «отсидел ли сотрудник восемь часов».

7. Карьерный и профессиональный рост. Удерживает не только вертикальный рост, но и возможность пробовать новое: переходить между проектами, ролями, технологиями. Прозрачные треки, менторство, доступ к обучающим ресурсам — всё это способствует внутренней мобильности, вместо перехода в другую компанию.

8. Экспертное признание и публичность. Всё больше IT-компаний поддерживают желание сотрудников делиться экспертизой. Это публикации в отраслевых изданиях, выступления на митапах, конференциях — с поддержкой компании, но сохранением авторства. Это не просто «личный бренд» — это ощущение признания и роста в профессиональном сообществе.

Высокая зарплата — это только начало. Настоящее удержание строится на уважении, развитии, доверии и смысле. Люди остаются там, где их ценят не как ресурс, а как личность и партнёра.

Какую роль играют возможности обучения и профессионального развития в удержании IT-специалистов?

Огромную. В IT всё меняется настолько быстро, что без постоянного обучения специалист просто начинает отставать от рынка. То, что ещё вчера было новым, сегодня уже становится стандартом. Яркий пример — технологии, связанные с ИИ: ещё несколько лет назад это была зона экспериментов, а сейчас они используются даже в рутинной автоматизации.

Компании, которые помогают сотрудникам развиваться, автоматически становятся привлекательнее — не только для найма, но и для долгосрочного сотрудничества.

Для начинающих специалистов (junior)

Обучение — это критический этап. Если компания помогает новичку освоиться, даёт доступ к базе знаний, выделяет наставника, организует разборы задач, спринты для обсуждения вопросов — такой сотрудник не просто учится быстрее, он и лояльность формирует с первых месяцев работы. Уровень вовлеченности напрямую зависит от того, насколько компания в него инвестирует.

Для специалистов уровня middle и выше

Тут уже важна глубина и возможность расширять экспертизу. Особенно востребованы:

- внешние курсы и сертификации по новым технологиям
- участие в профильных конференциях — не только как слушатели, но и как спикеры — тоже важно.
- внутренняя мобильность: возможность перейти на другой проект или попробовать себя в смежной роли
- менторство — как в роли наставника, так и ученика — даёт мощный толчок развитию. Это не только обмен опытом, но и рост: умение объяснять, задавать вопросы, принимать другую точку зрения — всё это развивает как хард, так и софт-скиллы.

Внутреннее обучение и культура обмена знаниями

Когда в компании есть внутренняя база знаний, регулярные встречи команд для разбора кейсов, технические митапы, практики code review с обучающим фокусом — это не просто обучение, это культура. Она формирует ощущение профессионального развития внутри компании, а не где-то «в другой жизни».

Обучение — это не бонус, а ключевой элемент удержания. Если человек чувствует, что может расти, пробовать новое, становиться сильнее как специалист — он не будет искать это в новой компании. Он будет строить карьеру внутри компании.

Как, по вашему мнению, уровень технологий, и организованность рабочих процессов влияют на удержание IT-специалистов?

Влияют напрямую. Сегодня для разработчика важно не только «что» он делает, но и «как» организована его работа. Если процессы хаотичны, нет инструментов, всё «на коленке» — такой специалист не задержится.

Современные технологии и методологии (Agile, Scrum, Kanban) позволяют:

- работать прозрачно и предсказуемо,
- чётко видеть цели и прогресс,
- избежать выгорания от бесконечных авралов.

Автоматизация — отдельный плюс: чем меньше рутинных задач, тем выше вовлечённость и интерес к работе. Confluence, Jira, таск-трекеры, аналитика и др инструменты — всё это снимает «боль» и высвобождает ресурс на настоящее развитие продукта.

Технологическая зрелость и чёткие процессы — это не только эффективность. Это ещё и уважение к труду специалиста. Именно такие условия удерживают сильных людей.

Личностные качества тимлидов влияют на удержание IT-специалистов?

Безусловно, тимлид — ключевой фактор удержания. Важно, чтобы он был именно лидером, а не просто техническим экспертом или формальным руководителем. Настоящий тимлид ведёт команду за собой, ясно показывает направление, активно вовлечён в задачи и процесс работы.

Он не ограничивается раздачей задач — он вовлечён в процесс, помогает разбирать сложные случаи, подсказывает решения, даёт честную и конструктивную обратную связь. Это руководитель, на которого можно опереться. С ним хочется работать, развиваться и оставаться в команде, где понимают и поддерживают.

Какие подходы к формированию эффективных команд вы считаете рабочими как в крупных, так и в небольших компаниях?

Главное — понять мотивацию каждого сотрудника и помочь ей реализоваться. Для этого нужен открытый диалог, а не формальные опросы с длинными анкетами, которые никто не хочет заполнять.

Лучше провести анонимный опрос всего лишь с одним вопросом «Что вам не хватает в компании?» — и слушать реальные ответы: кому-то нужна обратная связь, кому-то - обучение, кому-то - новые технологии, а кому-то — комфортное рабочее место или даже кофемашина.

После сбора информации HR и руководитель совместно анализируют данные и разрабатывают конкретные меры по улучшению условий работы и мотивации. Такой подход позволяет сотрудникам чувствовать, что их слышат и ценят, что снижает текучесть и повышает вовлечённость. Диалог и совместные усилия HR и менеджмента создают здоровую и продуктивную среду, в которой команда развивается и достигает результатов.

Как вы оцениваете влияние удалённой и гибридной работы на удержание IT-специалистов?

Гибкий формат работы сегодня — не привилегия, а норма, особенно, в IT. И именно он стал одной из ключевых причин, по которым специалисты остаются в компании. Возможность выбора формата — мощный инструмент удержания, если его грамотно адаптировать под потребности разных сотрудников.

Гибридный формат

Отлично работает для командной синхронизации, обмена опытом, мозговых штурмов и быстрых решений. Особенно полезен для:

- продуктовых команд, где важно совместно проектировать и обсуждать
- начинающих специалистов, которым нужен доступ к наставникам и обмен опытом

- ролей с высоким уровнем кросс-функционального взаимодействия

Гибрид даёт баланс: и живое общение, и возможность сосредоточенной удалённой работы. При этом важно, чтобы он был по-настоящему гибким, а не «по вторникам и четвергам все в офисе».

Удалёнка

Более уместна для экспертов и синьоров, которые хорошо самоорганизованы и не зависят от физического присутствия коллег. Такие специалисты ценят возможность работать из любой точки мира, концентрироваться на глубокой работе, а не на офисной суете. Для них удалёнка — это вопрос доверия и зрелости компании. Важно не просто «разрешить» удалёнку, а создать систему, в которой распределённые сотрудники чувствуют себя включёнными в процессы, получают обратную связь, участвуют в принятии решений.

Какие практики работы с удалёнными сотрудниками помогают снизить их отток?

Главный риск удалёнки — потеря связи с командой и компанией. Чтобы удержать таких сотрудников, важно создавать ощущение включённости и ценности.

Очные встречи

Даже 1–2 оффлайн-сбора в год (тимбилдинг, стратсессия, выездной корпоратив) резко усиливают лояльность. Это укрепляет связь и повышает мотивацию.

Регулярная онлайн-коммуникация

Регулярные демо, спринты, неформальные онлайн-встречи, общие чаты — всё это помогает сохранить ощущение команды и вовлечённости.

Обратная связь и развитие

Индивидуальные встречи, разговоры о целях и прогрессе, признание усилий — всё это критически важно. Сотрудники должны чувствовать: их замечают, с ними разговаривают, их вклад ценен.

Возможности влияния

Сотрудникам важно ощущать, что они не просто выполняют задачи, а могут участвовать в жизни компании: делиться идеями, влиять на проект (ну или заменить как-то это слово), развиваться, выступать, публиковаться с поддержкой компании.

Удалёнка требует системной работы. Чем больше точек включения в команду, тем выше шанс удержать специалиста.

Какие распространённые ошибки или заблуждения в стратегии удержания IT-специалистов вы могли бы выделить?

Самое опасное заблуждение руководителя — вера в то, что высокая зарплата сама по себе удержит сотрудника. Подход «заплатил и забыл» давно не работает.

Часто не уделяют должного внимания мотивации: не разбираются, что реально важно для каждого сотрудника, не работают с его профессиональным и личностным ростом.

Также распространённая ошибка — отсутствие регулярной обратной связи и признания. Люди хотят видеть, что их труд замечают и ценят, а не только получают деньги.

Без понимания и внимания к этим аспектам удержать сильных специалистов крайне сложно.

Итог:

Удержание IT-специалистов — это комплексный процесс, в котором важна не только достойная зарплата, но и уважение к человеку, признание его заслуг, прозрачность, возможности для роста и комфортные условия работы. Компании, которые инвестируют в развитие сотрудников, поддерживают открытость и гибкость, создают культуру доверия и смысла, выигрывают в борьбе за таланты и строят крепкие, успешные команды на долгие годы.

*Ирина Казакова,
IT Recruitment TeamLead в аутстаффинговой компании Smart IT

Редактор Л. Веселова · Корректор О. Сагун · Дизайн Н. Риль
Эксклюзивно для IT РЕВЬЮ

ИИ – применение в бизнесе, перспективы и развитие

Согласно исследованию MIT Sloan Management Review, почти 85% компаний считают, что ИИ позволит им получить или сохранить конкурентное преимущество. Однако лишь около 20% компаний внедрили ИИ в свои предложения или процессы, а только 5% сделали это в широком масштабе. Это указывает на значительный разрыв между амбициями и реальным внедрением ИИ в бизнесе. MIT Sloan Management Review

Антон Янушкевич,
Cryptemic Academy

Антон Янушкевич, основатель криптовалютной академии Cryptemic, отмечает:

«Компании, игнорирующие ИИ, рискуют остаться на обочине прогресса».

Эта мысль подчеркивает необходимость интеграции ИИ в бизнес-процессы для сохранения конкурентоспособности.

Как отметил Кай-Фу Ли, эксперт по ИИ:

«Наше будущее с ИИ будет создано нами и отразит выборы, которые мы сделаем, и действия, которые предпримем».

Эта цитата подчеркивает, что внедрение ИИ — это не просто технологический шаг, а стратегическое решение, определяющее будущее компании.

Текущие тренды использования ИИ в бизнесе: от гиперперсонализации до автономных роботов

В 2025 году искусственный интеллект (ИИ) перестал быть экспериментальной технологией и стал неотъемлемой частью бизнес-процессов во многих отраслях. От ритейла до логистики, от финансов до производства — ИИ трансформирует способы работы компаний, повышая эффективность, снижая издержки и открывая новые возможности для роста.

Ритейл: гиперперсонализация и прогнозирование спроса

Современные ритейлеры активно внедряют ИИ для анализа поведения покупателей и предсказания спроса. Согласно исследованию Analytics Insight, 80% руководителей розничной торговли ожидают, что их бизнес внедрит автоматизацию на основе ИИ к концу 2025 года. Exploding Topics

Amazon использует ИИ для прогнозирования спроса с точностью до 95%, что позволяет оптимизировать логистику и управление запасами.

Стартап Caper разработал «умные» тележки с ИИ-камерами, которые автоматически распознают товары в корзине, исключая необходимость ручного сканирования. Это не только ускоряет процесс покупок, но и собирает данные для дальнейшего анализа потребительского поведения.

Как отмечает Брайана Чифелли, старший директор по розничным медиа в Jellyfish: Skai

«Интеграция ИИ в розничные медиа ускоряется, с маркетплейсами, развивающими собственные креативные ИИ-студии и инструменты генерации инсайтов. Изучение и использование этих быстрых достижений имеет решающее значение в этой динамичной среде». Skai

Логистика: оптимизация маршрутов и автономные доставки

ИИ играет ключевую роль в оптимизации логистических процессов. Компания DHL использует ИИ для прогноза задержек, анализируя данные с датчиков транспорта и спутниковые снимки, что позволяет пересчитывать маршруты в реальном времени с учётом пробок и погодных условий.

Стартап Starship Technologies тестирует автономных роботов-доставщиков, которые уже работают в 20 университетских кампусах США, обеспечивая быструю и эффективную доставку товаров.

Кроме того, Volvo и DHL Supply Chain запустили беспилотные грузовики между Далласом и Хьюстоном, используя технологию Aurora Driver. Эти грузовики оснащены системами для контроля в случае отказа основных систем и оборудованы дальнобойными лидаром и высокоразрешающими камерами для почти 360-градусного обнаружения препятствий. Houston Chronicle

Финансы: борьба с мошенничеством и инвестиционные рекомендации

В финансовом секторе ИИ стал незаменимым инструментом для борьбы с мошенничеством и оптимизации инвестиционных решений. Mastercard использует генеративный ИИ для удвоения скорости обнаружения потенциально скомпрометированных карт, что позволяет быстрее защищать держателей карт и обеспечивать безопасность экосистемы. Mastercard

Сервисы вроде Betterment используют машинное обучение для создания персональных инвестиционных портфелей, учитывая риск-профиль клиента и рыночные тренды, что делает инвестиции более доступными и эффективными.

Как отметил Йохан Гербер, исполнительный вице-президент по безопасности и кибер-инновациям в Mastercard: Mastercard+2AP News+2WSJ+2

«Благодаря нашей ведущей в мире кибер-технологии мы теперь можем собрать пазл — усиливая доверие к банкам, их клиентам и всей цифровой экосистеме». Mastercard

Производство: предиктивный ремонт и цифровые двойники

На производственных предприятиях ИИ используется для предиктивного ремонта и создания цифровых двойников оборудования. Siemens внедрила ИИ-решения для предиктивного обслуживания, позволяющие компаниям предсказывать сбои до их возникновения, повышать время безотказной работы и снижать затраты благодаря ИИ-управляемым инсайтам. IT Brief Australia

Технология Digital Twin (цифровой двойник) позволяет создавать виртуальные копии станков для тестирования сценариев и оптимизации процессов, что сокращает простои и повышает производительность.

Роланд Буш, генеральный директор Siemens AG, подчеркнул важность интеграции физических и цифровых технологий:Wikipedia

«Цифровизация — это не о замене людей, а о расширении их возможностей». Wikipedia

Популярные ИИ-инструменты 2025 года: ChatGPT, DeepSeek и Perplexity AI

В 2025 году искусственный интеллект стал неотъемлемой частью бизнес-процессов, и выбор подходящих инструментов играет ключевую роль в эффективности компаний. Рассмотрим три ведущих ИИ-инструмента, которые активно используются в бизнесе.

ChatGPT: Мультимодальный помощник для бизнеса

ChatGPT от OpenAI, основанный на модели GPT-4o, представляет собой мощный инструмент для обработки текста, аудио и изображений. Он используется для создания контента, анализа данных и поддержки клиентов. Модель GPT-4o обеспечивает высокую скорость и точность, что делает ее привлекательной для различных бизнес-приложений.

Согласно данным OpenAI, GPT-4o предоставляет уровень интеллекта GPT-4, но работает быстрее и улучшает возможности в области текста, голоса и визуальных данных. Это позволяет компаниям создавать более персонализированные и эффективные решения для своих клиентов.

По данным Exploding Topics, ChatGPT.com получает около 5,19 миллиарда посещений в месяц, а количество еженедельных пользователей достигло 400 миллионов. OpenAI

планирует достичь 1 миллиарда пользователей к концу 2025 года. Exploding Topics+1The #1 Ranked AI Writer for SEO | SEO.AI+1

DeepSeek: Доступный ИИ из Китая

DeepSeek — китайский стартап, предлагающий мощные ИИ-модели по доступной цене. Их модель R1, выпущенная в январе 2025 года, быстро стала популярной, превзойдя ChatGPT в загрузках на App Store в США.

DeepSeek предлагает открытые модели, такие как V3, которые обеспечивают высокую производительность при низких затратах на обучение. Это делает их привлекательными для компаний, стремящихся внедрить ИИ без значительных инвестиций.

Кроме того, DeepSeek активно интегрируется в различные отрасли. Например, BMW планирует внедрить ИИ от DeepSeek в свои автомобили в Китае в 2025 году, а финансовые компании, такие как Tiger Brokers, используют их модели для анализа данных и принятия инвестиционных решений.

Perplexity AI: Интеллектуальный поисковый движок

Perplexity AI представляет собой интеллектуальный поисковый движок, предоставляющий точные и релевантные ответы на сложные запросы. Компания активно развивается, стремясь конкурировать с Google, и уже достигла 30 миллионов пользователей в месяц.

Perplexity AI также работает над созданием нового веб-браузера Comet, который будет интегрировать ИИ-функции, такие как сравнение цен и интеграция с различными сервисами, предоставляя пользователям более персонализированный опыт.

В условиях стремительного развития технологий искусственного интеллекта (ИИ) и его интеграции в различные сферы бизнеса, компании сталкиваются с необходимостью эффективного поиска и получения финансирования для реализации инновационных проектов. Традиционные методы подачи заявок на гранты часто оказываются сложными и трудоемкими, особенно для малых и средних предприятий.

В ответ на эту потребность появляются новые решения, такие как GrantiX, которые используют возможности ИИ для оптимизации процесса поиска и подачи заявок на гранты.

GrantiX: ИИ-платформа для оптимизации поиска грантов

GrantiX — это инновационная платформа, использующая технологии искусственного интеллекта для упрощения процесса поиска и подачи заявок на гранты. С помощью GrantiX компании могут быстро и точно находить подходящие грантовые возможности, соответствующие их профилю и потребностям. Платформа анализирует данные о компании и соотносит их с требованиями различных грантодателей, обеспечивая таким образом высокую степень соответствия и повышая шансы на успешное получение финансирования.

Кроме того, GrantiX предоставляет инструменты для автоматизации подготовки заявок, включая генерацию текстов, соответствующих требованиям грантодателей, и оптимизацию подачи документов. Это позволяет значительно сократить время и ресурсы, затрачиваемые на подготовку заявок, и повысить их качество.

Использование таких платформ, как GrantiX, становится важным шагом для компаний, стремящихся эффективно использовать возможности ИИ не только в своих продуктах и услугах, но и в процессах получения финансирования, что способствует ускорению инновационных разработок и развитию бизнеса в целом.

Эти инструменты демонстрируют разнообразие возможностей ИИ в бизнесе, от создания контента до анализа данных и поддержки клиентов. Выбор подходящего инструмента зависит от конкретных потребностей и целей вашей компании.

Развенчание мифов об ИИ в бизнесе

Вокруг искусственного интеллекта существует множество мифов, которые могут затруднять его внедрение в бизнес-процессы. Рассмотрим наиболее распространённые из них и предоставим актуальную информацию для их опровержения.

Миф 1: ИИ заменит всех сотрудников

Многие считают, что ИИ полностью заменит людей на рабочих местах. Однако исследования показывают, что ИИ скорее дополнит человеческие способности, автоматизируя рутинные задачи и позволяя сотрудникам сосредоточиться на более креативной и стратегической работе.

«ИИ изменит характер некоторых профессий, создавая новые возможности для людей

сосредоточиться на более значимых и творческих задачах», — утверждает представитель Microsoft. Source

Кроме того, согласно опросу PwC, более половины из 54 000 респондентов ожидают, что ИИ окажет положительное влияние на их карьеру в ближайшие пять лет. PwC

Миф 2: ИИ слишком дорогой для малого и среднего бизнеса

Существует мнение, что внедрение ИИ требует значительных инвестиций, доступных только крупным корпорациям. Однако с развитием технологий и появлением облачных решений ИИ стал доступен для компаний разного размера.

«Существуют доступные решения, особенно для малого и среднего бизнеса», — отмечает эксперт по ИИ.

Многие компании теперь предлагают ИИ-инструменты по модели «оплата по мере использования», что позволяет малым и средним предприятиям начать с небольших проектов и масштабировать их по мере необходимости.

Миф 3: ИИ требует идеальных данных для начала

Некоторые считают, что для эффективного использования ИИ необходимы исключительно качественные и структурированные данные. Однако современные ИИ-системы способны работать с неполными и неструктурированными данными, улучшая их качество по мере обработки.

«Модели ИИ часто разрабатываются для работы с несовершенными данными и могут улучшаться со временем, обучаясь на разнообразных входных данных», — утверждают специалисты. Fullstory

Миф 4: ИИ не имеет отношения к моему бизнесу

Некоторые предприниматели считают, что ИИ применим только в высокотехнологичных отраслях. Однако ИИ находит применение в различных сферах, от ритейла до финансов, помогая оптимизировать процессы и повышать эффективность.

«Многие инструменты, включая ChatGPT, предлагают ценные решения, независимо от размера или структуры компании», — отмечает эксперт. thealternativeboard.com

Миф 5: ИИ — это просто маркетинговый ход

Существует опасение, что компании используют термин «ИИ» как маркетинговый инструмент, не имея реальных технологий. Это явление известно как «AI-washing».Wikipedia

«AI-washing — это обманчивый маркетинговый приём, заключающийся в преувеличении роли ИИ в продукте или услуге», — говорится в исследовании.

Важно критически оценивать заявления компаний о применении ИИ и требовать подтверждения их реального использования.

Понимание и развенчание этих мифов поможет компаниям более уверенно подходить к внедрению ИИ, осознавая его реальные возможности и ограничения.

Преимущества и риски внедрения ИИ в бизнес

Внедрение искусственного интеллекта (ИИ) в бизнес-процессы открывает перед компаниями новые горизонты эффективности и инноваций. Однако вместе с преимуществами возникают и определённые риски, которые необходимо учитывать для успешной интеграции технологий.

Преимущества внедрения ИИ

Повышение эффективности и скорости процессов

ИИ способен автоматизировать рутинные задачи, сокращая время на их выполнение и снижая вероятность ошибок. Согласно исследованию McKinsey, компании, внедрившие ИИ, отмечают увеличение производительности на 20–30%.

Улучшение качества обслуживания клиентов

ИИ позволяет анализировать поведение клиентов и предлагать персонализированные решения, что повышает удовлетворённость и лояльность потребителей. Примером может служить использование чат-ботов на основе ИИ для круглосуточной поддержки клиентов.

Снижение операционных затрат

Автоматизация процессов с помощью ИИ позволяет сократить расходы на персонал и оптимизировать использование ресурсов. Отчёт PwC отмечает, что внедрение ИИ может привести к снижению затрат на 20–30%.

Ускорение принятия решений

ИИ способен обрабатывать большие объёмы данных в реальном времени, предоставляя аналитическую информацию для быстрого и обоснованного принятия решений.

Риски внедрения ИИ

Потеря рабочих мест

Автоматизация может привести к сокращению определённых должностей, особенно связанных с рутинными задачами. Однако, как отмечает Международный валютный фонд (МВФ), внедрение ИИ также создаёт новые рабочие места, требующие более высокой квалификации.

Этические и правовые вопросы

Использование ИИ вызывает вопросы, связанные с конфиденциальностью данных, предвзятостью алгоритмов и ответственностью за решения, принятые ИИ. Необходима разработка нормативной базы и этических стандартов для регулирования этих аспектов.

Зависимость от технологий и возможные сбои

Повышенная зависимость от ИИ может привести к уязвимости бизнеса в случае технических сбоев или кибератак. Важно обеспечить надёжность и безопасность ИИ-систем.

Неравномерное распределение выгод

Согласно отчёту МВФ, экономические выгоды от внедрения ИИ могут быть распределены неравномерно, что требует внимания со стороны политиков и бизнеса для обеспечения справедливости и устойчивости.

Понимание преимуществ и рисков внедрения ИИ позволяет компаниям принимать обоснованные решения и разрабатывать стратегии, направленные на максимизацию выгод и минимизацию потенциальных угроз.

Текущие тренды использования ИИ в бизнесе

В 2025 году искусственный интеллект стал неотъемлемой частью бизнес-стратегий, охватывая различные отрасли и бизнес-процессы. Рассмотрим ключевые направления применения ИИ:

Ритейл: гиперперсонализация и прогнозирование спроса

Машинное обучение анализирует поведение покупателей, предсказывая, какие товары будут востребованы. Например, нейросети Amazon прогнозируют спрос с точностью до 95%, оптимизируя логистику и складские запасы. Стартап Caper внедряет «умные» тележки с ИИ-камерами, которые автоматически распознают товары в корзине, исключая необходимость ручного сканирования.

Логистика: маршруты без пробок и роботы-курьеры

ИИ сокращает издержки на 20–30%, пересчитывая маршруты в реальном времени с учётом пробок и погоды. Компания DHL использует ИИ для прогноза задержек, анализируя данные с датчиков транспорта и спутниковые снимки. Стартап Starship Technologies тестирует автономных роботов-доставщиков, которые уже работают в 20 университетских кампусах США.

Финансы: фрод-детекция и роботы-советники

В банковской сфере ИИ стал незаменимым инструментом. Алгоритмы Mastercard анализируют 1,5 млн транзакций в секунду, выявляя мошенничество с точностью 99%. Сервисы вроде Betterment используют машинное обучение для создания персональных инвестиционных портфелей, учитывая риск-профиль клиента и рыночные тренды.

Производство: предиктивный ремонт и цифровые двойники

На заводах Siemens ИИ предугадывает поломки оборудования за недели до аварии, анализируя вибрации и температуру. Технология Digital Twin (цифровой двойник) позволяет

создавать виртуальные копии станков для тестирования сценариев. По данным PwC, это сокращает простои на 30% и повышает производительность на 25%.

Эти примеры демонстрируют, как ИИ трансформирует различные отрасли, повышая эффективность и снижая затраты. В следующем разделе мы рассмотрим популярные ИИ-инструменты 2025 года, которые помогают компаниям интегрировать ИИ в свои процессы.

Заключение: ИИ как стратегический актив бизнеса

Искусственный интеллект (ИИ) в 2025 году стал не просто технологией, а стратегическим активом, способным трансформировать бизнес-процессы, повышать эффективность и создавать новые возможности для роста. Компании, интегрирующие ИИ в свои стратегии, получают конкурентные преимущества, улучшая качество обслуживания клиентов, оптимизируя операции и ускоряя принятие решений.

Однако успешная интеграция ИИ требует не только технологических решений, но и изменений в корпоративной культуре, обучении персонала и управлении данными. Важно развенчивать мифы об ИИ, такие как страх перед заменой рабочих мест или представление о его дороговизне, и осознавать реальные возможности и риски, связанные с его внедрением.

Как отметил эксперт по ИИ: «Компании, которые сегодня интегрируют ИИ в свои процессы, завтра будут лидерами рынка. Не упустите шанс стать частью технологической революции».

Внедрение ИИ — это не просто технологический тренд, а необходимость для бизнеса, стремящегося к устойчивому развитию и инновациям.

*Антон Янушкевич, Основатель **Cryptemic Academy**

Редактор Л. Веселова · Корректор О. Сагун · Дизайн Н. Риль

Эксклюзивно для IT РЕВЬЮ

Уповать на то, что современный искусственный интеллект самостоятельно выстроит или оптимизирует бизнес-процессы, преждевременно

Владелец бизнеса должен понимать, какие функции должна выполнять автоматизация. «Если в компании происходит хаос и этот хаос автоматизировать, то это будет просто автоматизированный хаос.

ЧТОБЫ ПОЛУЧИТЬ ОТ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА КОРРЕКТНЫЙ ОТВЕТ, НУЖНО ПРАВИЛЬНО СОСТАВИТЬ ЗАПРОС, А ДЛЯ ЭТОГО ИИ НУЖНО НАСТРОИТЬ, ОБУЧИТЬ И СФОРМИРОВАТЬ.

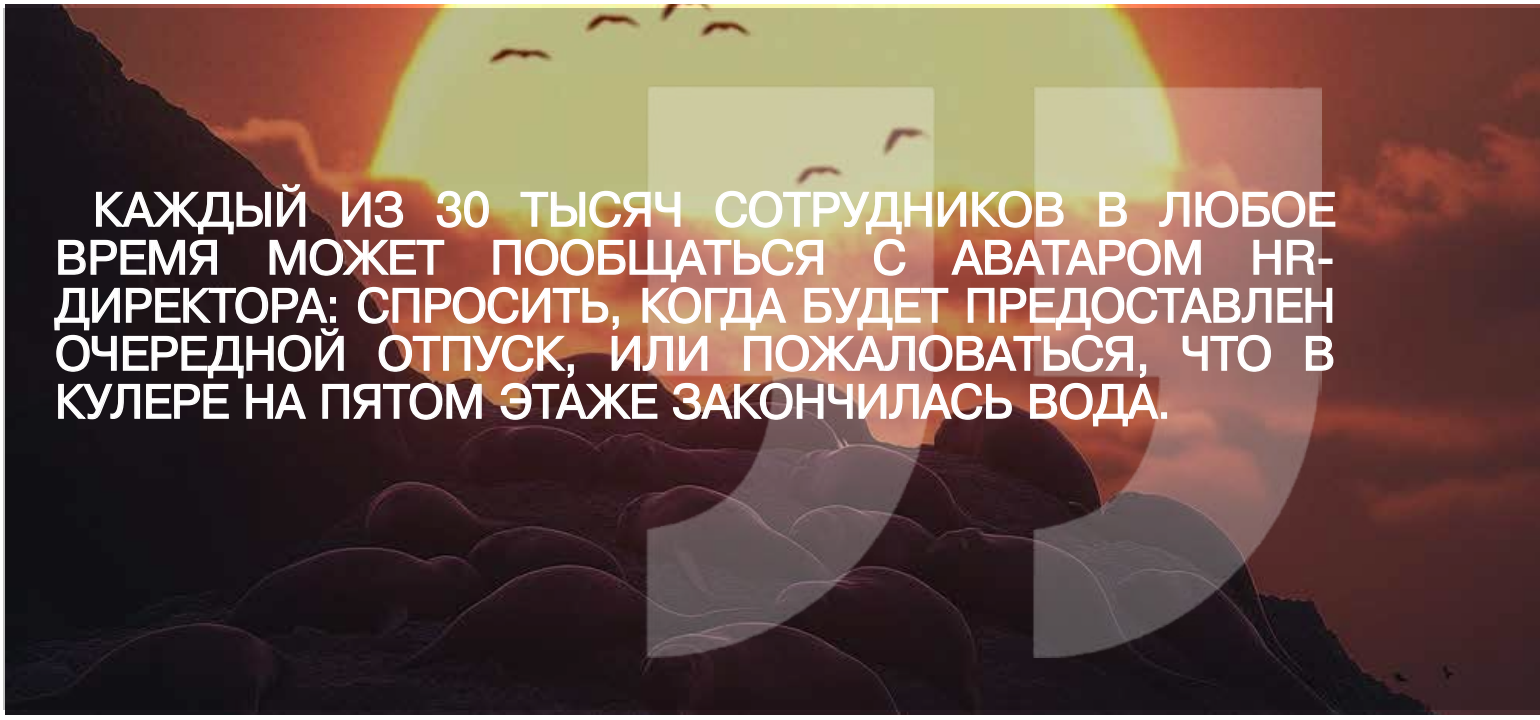
Ирина Шамехо,
«Большие продажи»

За этим всегда стоит человек».

Наибольший интерес в условиях кадрового голода вызывает возможность замены сотрудников, выполняющих рутинные операции, что весьма эффективно с экономической точки зрения. Например, канадская холдинговая компания Eberts Holdings смогла вдвое уменьшить количество персонала. Альфа-банк благодаря подобным инструментам сократил число кассиров со 120 тысяч до 50 тысяч.

Еще одним направлением, требующим более творческого подхода, является использование чат-ботов в общении как с клиентами, так и внутри компании. Однако поспешные шаги могут вызвать нежелательную для её репутации реакцию, в чём многие уже убедились на собственном опыте. В сфере HR, например, не каждый кандидат настроен общаться с искусственным представителем потенциального работодателя: «Почему меня не пускают к принимающему решение человеку?» — и доверие к компании падает. И в этом случае важная роль принадлежит разработчику технологии виртуального общения.

В качестве примера того, как чат-бот способен повысить лояльность сотрудников, можно привести заводы «Россельмаш» и «Северсталь», где

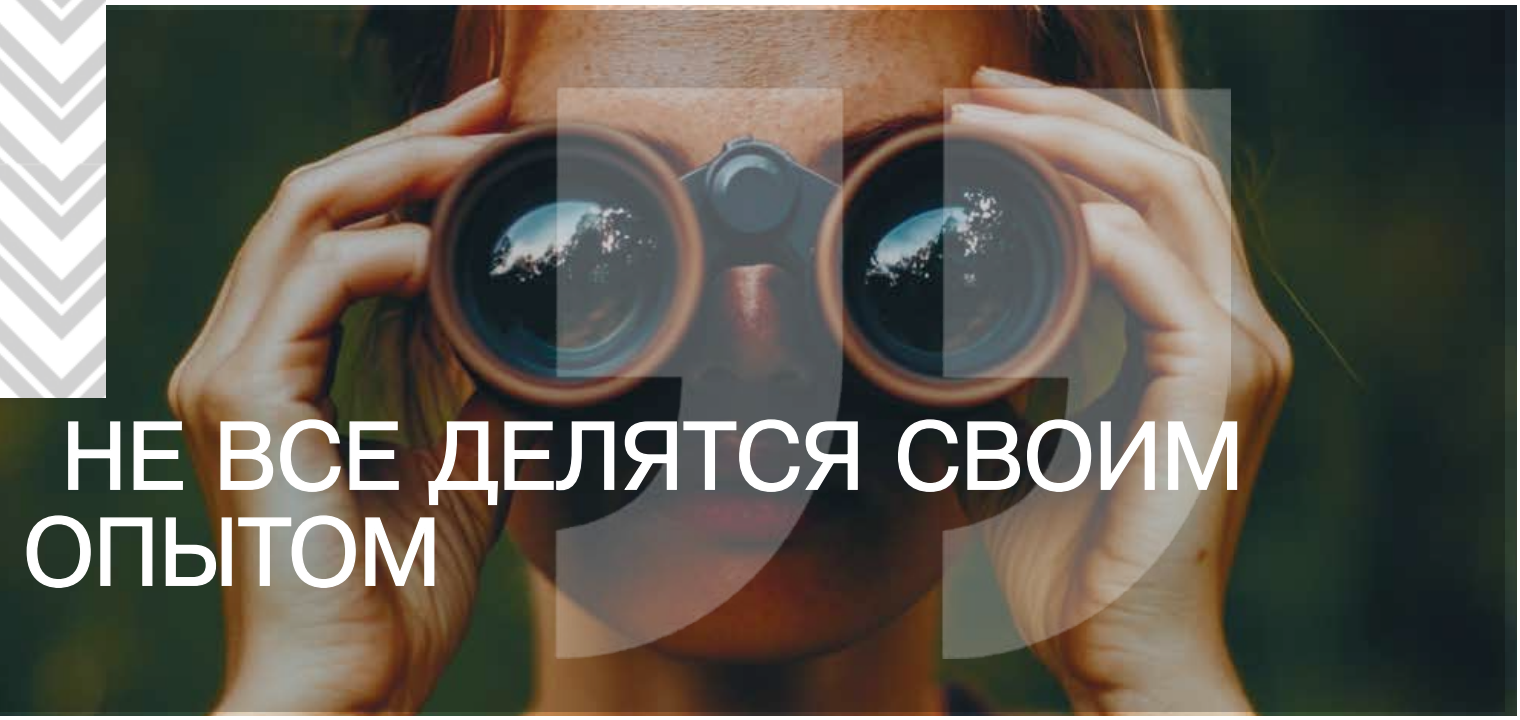


Ответ следует незамедлительно, и люди очень довольны, что улучшает общую рабочую атмосферу компании.

Очень популярны обучающие чат-боты как для клиентов, так и для сотрудников компаний, когда ИИ выполняет роль тьютора: выдаёт задания, напоминает о сроках, поддерживает обучающегося, даёт подсказки.

Сбер доверяет ИИ ещё более тонкую работу — профайлинг. Так, например, в ходе анализа открытой переписки персонала он предсказывает возможную дату подачи сотрудником заявления об увольнении. Однако и здесь всё зависит от человека, который ставит задачу.

Данные технологии используют многие компании, но, естественно,



НЕ ВСЕ ДЕЛЯТСЯ СВОИМ ОПЫТОМ

*Ирина Шамехо, соосновательIT-компании **«Большие продажи»**

Редактор Л. Веселова · Корректор О. Сагун · Дизайн Н. Риль

Эксклюзивно для IT РЕВЬЮ

Внедрение ИИ не стало “увольнением людей

Как художник превратил 12 человек в троих: мой путь повышения эффективности с помощью ИИ

Татьяна Кенцис,
@izo.project»

Многие воспринимают художника как одиночку с мольбертом, красками и вдохновением. Но современное художественное производство, особенно в сфере иллюстрации и комиксов, — это сложный, многоэтапный процесс, в котором задействованы десятки компетенций: от сценарной разработки до финальной верстки. Я, как художница и куратор собственного проекта, за годы выстроила команду из 12 человек: одни занимались идеями и сторителлингом, другие — литературной обработкой текста, третьи — проверкой грамотности, четвёртые — черновыми зарисовками, пятые — цветом, шестые — фонами и так далее.

Но всё изменилось с приходом инструментов на базе искусственного интеллекта. Я начала с простого — редактура текстов: теперь я использую ИИ для корректуры, стилистической вычитки и улучшения читаемости. Далее — генерация идей. Брейншторминг, на который раньше собиралась целая команда, теперь может проходить даже ночью, в одиночестве, но с участием умного собеседника. ИИ может быстро предложить десятки сюжетных ходов, необычных поворотов или визуальных решений, которые раньше приходилось выдумывать коллективно.

Что касается иллюстраций — здесь особенно ощутим эффект. Вместо шести разных специалистов, каждый из которых работал на своём этапе (композиция, свет, текстуры, цвет, фон, мелкие детали) — теперь достаточно двух-трёх человек: один создает первичную генерацию с ИИ, второй доводит до стиля студии, третий проверяет соответствие ТЗ. Это не замена человеку, это усиление. Я бы даже сказала: это экономия не только времени и бюджета, но и психологических ресурсов.

Процесс, который раньше длился 3–4 недели и требовал участия десятка людей, теперь может быть завершён за 5–7 дней с командой из трёх. Мы не потеряли в качестве, а в некоторых случаях даже выиграли — благодаря свежести решений и отсутствию “замыливания глаза”.

Внедрение ИИ не стало “увольнением людей” — это был стратегический переход к новой форме взаимодействия. Те, кто остался в команде, стали гораздо более многозадачными, гибкими, и получили больше свободы для творчества, а не рутины. В условиях современной экономики это стало ключом к устойчивости проекта.

СЕГОДНЯ ЭФФЕКТИВНОСТЬ МОЕГО ТВОРЧЕСКОГО “ПРОИЗВОДСТВА” ВЫРОСЛА ПОЧТИ В ТРИ РАЗА, ПРИ ЭТОМ ЧЕЛОВЕЧЕСКИЙ ФАКТОР СТАЛ НЕ СЛАБЫМ ЗВЕНОМ, А ЦЕНТРОМ ПРИНЯТИЯ РЕШЕНИЙ,

наполненным вдохновением, смыслом и эстетикой. Именно поэтому я считаю, что интеграция ИИ в творческую сферу — это не про технологии. Это про гуманизм.

*Татьяна Кенцис, Основатель @izo.project и художник с 20 летним стажем

Редактор Л. Веселова · Корректор О. Сагун · Дизайн Н. Риль

Эксклюзивно для IT РЕВЬЮ

Искусственный интеллект в бизнесе: революция, которую вы пропускаете

Пока большинство компаний по-прежнему воспринимают искусственный интеллект как модную опцию или «игрушку для продвинутых», бизнес-среда переживает системную трансформацию. ИИ — это не про завтра. Это про сегодня. А те, кто не адаптируется, рискуют выйти из игры — тихо и незаметно.

Алина Новикова,
Winner.Team.

Темпы внедрения ИИ-технологий сопоставимы с тем, как интернет в 90-х изменил ландшафт деловой активности. Только на этот раз адаптационного люфта нет: интерфейсы обновляются буквально на следующий день после выпуска обучающих курсов. Речь уже не о планировании на квартал, а о ежедневной калибровке процессов.

ИИ — это не только про технологии. Это про эволюцию управленческого мышления

Современные нейросети не ограничиваются генерацией текстов. Они:

- анализируют переговоры;
- распознают модели поведения сотрудников;
- оценивают тональность и мотивационные маркеры;
- проводят базовую аналитику;
- участвуют в принятии решений.

ИИ уже работает во всех отраслях — от HR и PR до продаж, маркетинга, журналистики, копирайтинга, стратегии, финансов, строительства и медицины. Это больше не «где-то далеко», это часть операционной реальности самых разных команд.

И всё это — с минимальным вмешательством человека. Однако потенциал нейросетей реализуется лишь в том случае, если пользователь умеет правильно ставить задачи и интерпретировать ответы. ИИ — это не магия. Это усилитель. Он масштабирует ваш стиль мышления, умножая сильные стороны и оголяя слабые.

Согласно исследованиям Гарвардской школы бизнеса, MIT и McKinsey, сотрудники, использующие ИИ, демонстрируют рост продуктивности на 200–300% по сравнению с коллегами. Так формируется новый тип профессионалов — superworkers — сотрудники, чья цифровая прокачка обеспечивает кратный рост операционной эффективности.

Компании, готовые к будущему, инвестируют в обучение уже сегодня

В 2023 году IBM приостановила набор 8000 человек: функции этих сотрудников перераспределили между ИИ-инструментами и уже работающими специалистами, обученными новым технологиям. Это не сокращение — это перераспределение ресурса в сторону продуктивности.

В США масштабное внедрение ИИ в бизнес-практики началось ещё два года назад. Корпорации в массовом порядке обучали весь персонал — от административного блока до топ-менеджмента. В России этот этап только начинается. Но отставание недопустимо. Как писал Льюис Кэрролл: «Нужно бежать со всех ног, чтобы только оставаться на месте».

ИИ — это не просто про бизнес. Это про возможности, которые раньше казались недоступными

Я обучаю специалистов самых разных профессий — от PR-директоров и врачей до владельцев малого бизнеса. Общий результат: экономия от 10 до 15 часов в неделю, рост качества решений и появление ресурса для тех проектов, до которых годами не доходили руки.

Примеры:

Участница марафона создала нейро-консультанта по подготовке к ОГЭ/ЕГЭ. По отзывам — эффективнее живых преподавателей.

Другая разработала ИИ-ассистента по питанию для диабетиков 1 типа — социально значимый проект, ранее невозможный из-за ограниченности ресурсов.

И это не исключения, а новая реальность.

Что уже сегодня автоматизируют бизнесы с помощью ИИ:

- написание и корректировка должностных регламентов;
- протоколирование совещаний с анализом вовлеченности;
- формирование портретов ЦА и SWOT-анализ;
- генерация и адаптация скриптов продаж;
- первичный отбор кандидатов на основе резюме;
- аналитика по данным, анкетам, открытым источникам.

ИИ убирает человеческий фактор, снижает риски субъективности и позволяет получать системный, воспроизводимый результат. Это не просто про эффективность — это про профессиональный уровень компании.

ИИ не заменит людей. Но он точно заменит тех, кто не готов меняться

ИИ не умеет чувствовать, не создаёт смыслы и не формирует интуитивные выводы. Но он умеет обрабатывать большие массивы данных, анализировать паттерны и выдавать прогнозы. Следовательно, сотрудники, которые выполняют рутинные, повторяющиеся задачи без добавленной ценности, будут вытеснены первыми.

Ключевой вызов — научиться быть не просто исполнителем, а оператором ИИ. Тем, кто мыслит гибко, ставит задачи точно и умеет интерпретировать результат.

С чего начать?

Не стоит изучать сотни нейросетей. Достаточно проанализировать свои процессы и выбрать 1–2 инструмента, которые решат конкретные задачи: автоматизация, аналитика, генерация контента, структурирование данных. Далее — дело практики и точечной настройки.

ИИ — это новая форма грамотности. И уже сегодня она стала базовым требованием к специалисту любой сферы.

Вывод:

Революция произошла. Вопрос не в том, вступать в неё или нет — вопрос, на каком уровне вы в ней участвуете. Потому что в условиях новой реальности выигрывает не тот, кто больше работает, а тот, кто умеет мыслить быстрее, шире и стратегичнее. А значит — с ИИ.

И да: выбор по-прежнему начинается с себя.

*Алина Новикова, Эксперт по нейросетям, сооснователь агентства по внедрению ИИ-решений и кадрового агентства Winner.Team.,
Консультант и бизнес-тренер для корпоративных клиентов в сфере EdTech и HR-tech

Редактор Л. Веселова · Корректор О. Сагун · Дизайн Н. Риль

Эксклюзивно для ITРЕВЬЮ

Автоматизация складов как таковая перестаёт быть конкурентным преимуществом

Виталий Янко

Согласно исследованию MIT Sloan Management Review, почти 85% компаний считают, что ИИ позволит им получить или сохранить конкурентное преимущество. Однако лишь около 20% компаний внедрили ИИ в свои предложения или процессы, а только 5% сделали это в широком масштабе. Это указывает на значительный разрыв между амбициями и реальным внедрением ИИ в бизнесе. MIT Sloan Management Review

1. Роботы для логистики и автоматизация складов

Не так давно в СМИ про цифровизацию отраслей реального сектора мне задавали вопрос про лучший выбор роботов для логистики. С 2016 года я был инвестором и «играющим тренером» (коммерческим директором) в группе компаний RobotikUm, развивавшую промышленную и образовательную робототехнику. Когда в 2021 году я вышел из акционеров этих проектов, то для себя рассматривал возможности вложиться в складских роботов (проект Киберсклад) и в готовые роботележки всяких форматов, которые нуждались в масштабировании. Не хочу называть сейчас конкретных поставщиков WMS систем (warehouse management, управление складами) и складских роботов. Не в них соль вновь – а в управляющем ПО на стыках, повышающем эффективность.

Вообще, автоматизация складов как таковая перестаёт быть конкурентным преимуществом — это уже необходимое условие для устойчивой работы логистических цепей.

Судя по запросам на роботележки (я изучал этот рынок в 23-24 годах с целью инвестирования от лица крупного холдинга), всё больше российских компаний делают ставку на внедрение WMS-систем, интеллектуальных трекеров, робототехники и компьютерного зрения. По оценкам логистических операторов, за последние 3 года количество складов с частичной или полной автоматизацией выросло в среднем на 25–30%. Моя оценка такова, что у крупнейших сетей доля роботизации распределительных центров уже выше 70%.

Но один из самых острых вызовов в логистике сегодня — управление запасами в условиях регуляторных изменений и высокой номенклатурной нагрузки.

Введение обязательной маркировки товаров (например, в рамках «Честного знака») требует высокой точности при идентификации продукции, а человеческий фактор, особенно в процессе сканирования, часто становится причиной ошибок. Сотрудники сталкиваются с необходимостью считывания множества кодов: на приёмке, при подборе товара, при инвентаризациях, при отгрузке. Если сканер не может распознать затёртый, засвеченный или повреждённый код — товар уходит в «зависание», искажается учёт, теряется время. Управляющие программы, стоящие на бортах складских робопогрузчиков и роботележек, обладают возможностью ориентации в пространстве, но редко работают с массовой идентификацией товаров. Без точных и быстрых алгоритмов захвата данных даже самый современный робот становится просто дорогим переносчиком груза на тележке.

А склады ищут для себя универсальные алгоритмы сканирования вместо ушедших с рынка швейцарских авторов ПО.

Это решения, способные не просто считать QR- или штрих-код, а “увидеть” его в любых условиях: даже при плохом освещении, с изгибами упаковки, с большим количеством кодов в кадре. Современные алгоритмы компьютерного зрения позволяют фиксировать сразу несколько кодов, вести их трекинг даже при смещении камеры, исключать дубли и давать корректную привязку к учётной системе — без необходимости в спецоборудовании. В целом эту проблему решает входящий в SPB Founders петербургский стартап RuScanna, который я встречал в академии ИИ проектов компании Selectel. Они делают множественное сканирование кодов в условиях склада или торгового зала.

Другой гранью быстрой работы с видеопотоком (ниже – почему это важно) является компания Fastvideo из Дубны, которая умудряется “обгонять” скорость распаковки видеосигнала на оконечных устройствах типа кабины безлюдного экскаватора и встроенного в робот-экскаватор

управляющего компьютера, и за этот счёт снижать стоимость навесного оборудования и быстрее обрабатывать видеосигнал, что повышает точность работы машины и безопасность работ. Более того, возможность оффлайн-сканирования с обычного смартфона снимает потребность в дорогостоящих ТСД и повышает мобильность персонала.

Несколько крупных логистических компаний (включая крупнейшего оператора Северо-запада Модуль) обладают своими решениями сканирования на грузовых терминалах, которые установлены на защищённые смартфоны сотрудников. Но вовне их не поставляют, насколько мне известно. Будущее складской логистики — это все же адаптивные системы, в которых ключевую роль играют именно алгоритмы, а не оборудование. Это особенно важно на фоне дефицита персонала и нормативных “штормов”. Поэтому мы вернулись к идее, что именно компьютерное зрение на конечных устройствах с целями быстрой обработки и распознавания видео сигнала — центральный узел всей автоматизации склада/терминала. И улучшение именно этого элемента способно дать наибольший экономический и операционный эффект. Именно туда продолжаю инвестировать.

2. Цифровизация добывающей отрасли

Такой же вопрос мне задавали на днях и в духе, «почему в России буксует цифровизация добывающей отрасли». Меня спрашивали, согласен ли я с тем, что в России есть проблемы с цифровизацией добывающей отрасли (на предприятиях, которые занимаются добычей сырья, производством и переработкой материалов и энергии).

Мы же с партнерами инвестбутика SPB Founders считаем, что с цифровизацией у добывающей отрасли проблем нет. У каждого крупного бизнеса и корпорации в добыче еще лет 5-7 назад появилась стратегия цифровизации (зачастую также называют стратегией цифровой трансформации). Сейчас, куда ни посмотри, в каждой крупной компании есть свои внутренние R&D-подразделения, которые занимаются in-house разработкой цифровых продуктов, но чаще всего это – микросервисы, которые (как правило) разворачиваются внутри собственной экосистемы продуктов и предназначены для пользования исключительно внутри (кастомизация под специфику отрасли и компании). Если посмотреть на рынок вендоров, то практически у каждого уже есть в портфеле продукты, которые направлены на цифровизацию бизнес-процессов, которые присущи добывающей отрасли. Спрос со стороны добывающих компаний и предложения от вендоров - на рынке есть, это факт. Главным барьером, наверняка, остается специфика отрасли и тяжелое «legacy» (устаревшее ПО – можно назвать это «техническим долгом», в какой-то степени). Да и сами по себе B2B-продукты для Larger Enterprise не могут быть универсальными и не могут быть внедрены в производственный процесс, будто “из коробки”. Таким продуктам зачастую требуется кастомизация с длительной подготовкой до момента

ввода в эксплуатацию: предпроект, PoC (proof of concept, доказательство работоспособной концепции), консалтинговый проект, техаудит и так далее – казалось бы, что это просто порядок дел на рынке, но у добывающих компаний (особенно крупных и госкорпораций) ранее были зарубежные узкоспециализированные отраслевые цифровые продукты, на которых чуть ли не десятки лет работал весь операционный бизнес. Более-менее все нормально в отраслях топливно-энергетического комплекса, поскольку они были одними из первых кто пошел в цифровизацию, но в других конечные клиенты испытывают большие проблемы из-за довольно большой специфичности бизнес-процессов и технологий. Можно, к примеру, взять какой-нибудь MES – и конечная стоимость внедрения (и лицензия первого года) у нефтегаза будет дешевле, чем у той же алмазодобывающей – это обусловлено глубокой кастомизацией под заказчика, потому что у нефтегаза инфраструктура в порядке, и они давно работают на fine tuning всего внутри, чего не скажешь о компаниях – добывающих, к примеру, золото или алмазы. Причина – нет бенчмарка в РФ, не на кого равняться и не с кем конкурировать.

* MES-система (Manufacturing Execution System, система управления производственными процессами) — это программный комплекс для оперативного планирования и управления производством продукции.

В заключение, хочу сказать, что перспективы у отечественного ПО на внутреннем рынке есть. Грануляция и «закукливание» проектов мы наблюдаем только в области разработки «в стол», где нет профи, успевших цифровизовать компании сферы логистики или промышленности на стороне самих предприятий. А «инфоцыганство» от IT в реальном секторе в 2026 году точно не купят

*Виталий Янко, Коммерческий директор в ИТ с 2007 года, в венчуре с 2019 года, основатель сообщества успешных ИТ экспортеров ExportNow, консультант по монетизации ПО, с 2007 года коммерциализует российские разработки в качестве коммерческого директора софтверных и финтех-компаний

Беседовала М. Удалова
Редактор Л. Веселова · Корректор О. Сагун · Дизайн Н. Риль

Эксклюзивно для ITРЕВЬЮ

ПРАКТИЧЕСКИЙ ДЕЛОВОЙ ЖУРНАЛ

Мастер Продаж

№ 4 / 2025

ОБЗОРЫ · КОММЕНТАРИИ · ПРАКТИКА

ИЗДАТЕЛЬСТВО ЖУРНАЛА

Запомните: любые переговоры — это продажа, но не любая продажа — это переговоры!

Сергей Былинкин

ИНФОРМАЦИОННО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

ЕЖЕКВАРТАЛЬНЫЙ ЖУРНАЛ

ДЕЛОПРОИЗВОДСТВО

www.TOP-PERSONAL.RU

(июль-сентябрь)

№3
2025

В номере:

При поддержке:

УПРАВЛЕНИЕ ПЕРСОНАЛОМ

ИЗДАТЕЛЬСТВО ЖУРНАЛА
УПРАВЛЕНИЕ ПЕРСОНАЛОМ

Коммерческие споры

№ 2 / 2025

Разделяйте деловые и личные отношения

Елена Родионова