

ПРАКТИЧЕСКИЙ ДЕЛОВОЙ ЖУРНАЛ

РЕВЬЮ

ОБЗОРЫ · КОММЕНТАРИИ · ПРАКТИКА

№2/2026



**Юлия
Мицкевич**
CODE



**Денис
Коннов**
Kinescope



**Евгений
Былинкин**
WeBrain



**Федор
Задков**
gvozdz.org



**Злата
Похалуева**
Бизнес-тренер



**Максим
Гаёв**
AMI-Sales



**Дмитрий
Ушаков**
«Гладиаторы ИБ»



**Елена
Назарова**
ItFox



**Дмитрий
Тулупов**
консультант



**Александр
Ожерельев**
NeoGraph.tech



**Наталья
Абрамова**
эксперт ИИ

Содержание

- 3 **ЦЕНЫ НА СОФТ**
Сколько стоит AI-софт для digital-команд и что он реально даёт бизнесу
Юлия Мицкевич, KODE
- 7 **ВИДЕОХОСТИНГ**
Видеохостинг для бизнеса: как считать расходы и не переплачивать
Денис Коннов, Kinescope
- 14 **ПЛАТФОРМЫ**
Как выбрать платформу для запуска сайта под свой бизнес
Евгений Былинкин, WeBrain
- 19 **СОФТ**
Как мы продаём gvozd.org
Федор Задков, gvozd.org
- 21 **HR&SOFT**
Запрос о том какой именно софт вам нужен – это компас вашей удачи в поиске софта
Злата Похалуева
- 25 **ЦЕНЫ НА СОФТ**
Цены на софт для бизнеса в IT: как посчитать эффективность
Максим Гаёв, AMI-Sales
- 31 **КИБЕРБЕЗОПАСНОСТЬ**
Как чашка кофе может спасти компанию от хакера
Дмитрий Ушаков, «Гладиаторы ИБ»
- 39 **ВИДЫ АУТСОРСИНГА**
IT-аутсорсинг-2026: кто на коне, а кто ушел в вайб-кодинг?
Елена Назарова, ItFox
- 44 **КИБЕРБЕЗОПАСНОСТЬ**
Кейсы аудитов кибербезопасности различных компаний
Дмитрий Тулупов, консультант по Кибербезопасности и ИИ
- 50 **ЦЕНЫ НА СОФТ**
Цены на софт для бизнеса в IT – как посчитать эффективность
Александр Ожерельев, NeoGraph.tech
- 56 **КИБЕРБЕЗОПАСНОСТЬ**
Искусственный интеллект в системе документооборота и управления корпоративными процессами
Наталья Абрамова, эксперт по искусственному интеллекту

Издательский дом представляет ведущие деловые журналы

Подписные индексы:

По объединённому каталогу ГК РФ

Журнал издаётся при участии Историко-архивного института Российского государственного гуманитарного университета и Всероссийского научно-исследовательского института документоведения и архивного дела Росархива



Официальный адрес
TR@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.

Издательство не несет
ответственности за ущерб,
нанесенный в результате
использования, неиспользования
или ненадлежащего
использования информации,
содержащейся в настоящем
издании.

Перепечатка материалов (полная
или частичная) допускается только
с письменного разрешения
редакции.

Издатель: ООО «Топ-Персонал»
с 2011 г.

Подписано в печать 14.04.2026.
Формат 60x90 1/8.

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

Иллюстрации созданы ИИ:
Midjourney

© «ИТ Ревью», 2026.

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

Компании активно внедряют AI, но не до конца понимают его экономику: сколько это стоит и какой эффект даёт на практике ...

>3

Юлия Мицкевич,
операционный директор международной IT-компании KODE

Главная ошибка — представлять видеохостинг как IT-расход. Это расход на учебную инфраструктуру, и считать его нужно в логике стоимости обучения на одного сотрудника...

>7

Денис Коннов,
директор по маркетингу Kinescope

Выстроенные бизнес-процессы гораздо важнее оболочки...

>14

Евгений Былинкин,
руководитель WeBrain

Этой аудитории не нужны общие фразы. Им нужны конкретные инструменты, которые решают их ежедневные боли...

>19

Федор Задков,
gvozdz.org

Почему мы отсеяли “тяжелый” софт Первое – стоимость. Оплата за каждую лицензию....

>21

Злата Похалуева,
Бизнес-тренер ведущих бизнес-школ по курсу «Управление персоналом»,
автор и ведущий курса «Профессиональный рекрутер»

Сколько стоит AI-софт для digital-команд и что он реально даёт бизнесу

По данным отчёта AI Index 2025 Стэнфордского университета, 78% компаний уже используют искусственный интеллект хотя бы в одной бизнес-функции — от разработки до маркетинга. При этом, по исследованию McKinsey, лишь около 39% компаний могут напрямую связать использование AI с финансовым результатом.

Компании активно внедряют AI, но не до конца понимают его экономику: сколько это стоит и какой эффект даёт на практике. Чтобы разобраться, мы собрали данные сотрудников нашей digital-команд о том, какие AI-инструменты они используют, для каких задач и как это влияет на рабочие процессы.

Как digital-команды используют AI в работе

Внутренний опрос показал, что AI уже стал частью повседневной работы: 68% сотрудников используют его ежедневно, ещё 10% — несколько раз в неделю.

Чаще всего AI применяют для задач, связанных с обработкой информации. 90% сотрудников используют его для ресёрча, поиска решений и обучения. По сути, AI становится альтернативой поисковым системам и документации: вместо десятков



Юлия
Мицкевич

операционный директор
международной IT-компании
KODE

вкладок специалист получает структурированный ответ и может уточнять его в диалоге. Также AI активно используется в технических задачах:

60% сотрудников применяют его при разборе инцидентов для анализа логов, поиска причин ошибок и понимания сложных системных сообщений

50% — в работе с кодом, в том числе для генерации тестов, шаблонных решений и анализа кода

40% — для переводов и интернационализации, что особенно важно в проектах с несколькими языками

70% разработчиков уже используют AI и в основном стеке, а 60% — для изучения новых технологий и пет-проектов. Это показывает, что AI начинает влиять не только на скорость работы, но и на обучение специалистов.

По оценке команды, AI экономит около 5–20% времени на типовых задачах. Это не кратный рост эффективности, но стабильное ускорение повседневной работы.

Сколько стоит AI для команды

В реальной работе команда использует несколько инструментов: ChatGPT, Claude, Gemini, Cursor, DeepSeek и Gamma. При этом структура затрат отличается от классического корпоративного софта:

60% сотрудников используют бесплатные версии AI-сервисов

платные инструменты используются точечно, под конкретные задачи

часть сервисов используется с одного аккаунта несколькими сотрудниками

Основные платные инструменты:

ChatGPT — \$20 в месяц

Claude / Gemini — \$20

Gamma — \$10–20

В результате даже при активном использовании расходы остаются относительно низкими. В большинстве случаев базовый AI-стек обходится примерно в \$20–80 на сотрудника в месяц, а при частичном использовании значительно дешевле.

Важно, что в отличие от традиционного корпоративного ПО, здесь нет больших затрат на внедрение, интеграцию и поддержку. Большинство инструментов начинают приносить пользу сразу после подключения.

Экономический эффект от AI складывается не из одного крупного улучшения, а из множества небольших ускорений.

Как посчитать окупаемость AI

Экономика AI становится понятной, если перевести её в рабочее время. Если команда из 10 человек использует AI-инструменты стоимостью \$20 на человека, расходы составляют \$200 в месяц.

При загрузке 176 часов в месяц даже минимальная экономия в 5% даёт около 9 часов на сотрудника или 90 часов на команду. Это не выглядит как прорыв на уровне одной задачи, но на уровне команды превращается в значительный объём высвобожденного времени.

Даже без точного расчёта стоимости часа видно, что стоимость AI-инструментов сопоставима с несколькими часами работы специалиста, а экономия — с несколькими рабочими днями команды.

Пример: ускорение разработки. Разработчики используют AI для автодополнения кода, генерации тестов и написания шаблонных частей логики. В среднем типовая задача занимает около 8 часов, а с использованием AI — около 6,5–7 часов. При команде из 5 разработчиков и 40 подобных задачах в месяц это даёт экономию порядка 60 часов. Даже при средней стоимости часа это эквивалентно десяткам тысяч рублей.

Почему эффект от AI не всегда виден сразу

Один из важных выводов — AI не даёт мгновенного роста эффективности на уровне всей компании. На этапе внедрения команда тратит время на выбор инструментов, тестирование сценариев использования, обучение сотрудников, проверку результатов.

На коротком промежутке может казаться, что AI не экономит время, а наоборот увеличивает его расход. Однако по мере накопления опыта ситуация меняется: сотрудники начинают использовать AI точно — там, где он действительно ускоряет работу. Именно в этот момент появляется реальный экономический эффект.

Что это означает для бизнеса

AI-инструменты стоят десятки долларов в месяц на сотрудника, но позволяют экономить часы рабочего времени каждую неделю. При этом эффект не всегда проявляется мгновенно, он накапливается по мере того, как команда учится использовать AI в нужных задачах.

Даже при 5–10% экономии времени такие инструменты окупаются быстрее, чем большинство корпоративного софта. Особенно в digital-командах, где значительная часть работы связана с разработкой и анализом информации. Поэтому AI постепенно становится не экспериментом, а базовым инструментом, который влияет не только на скорость работы, но и на экономику проектов.

*Юлия Мицкевич,
операционный директор международной IT-компании **KODE**

Эксклюзивно для **ITРЕВЬЮ**

**ВМЕСТЕ С ITREVIEW ВЫ ПОЛУЧАЕТЕ В ПОДАРОК
ОТ ИЗДАТЕЛЯ ЖУРНАЛЫ В ЭЛ ВЕРСИИ:**



ПОЧТА 7447273@VK.RU

Видеохостинг для бизнеса: как считать расходы и не переплачивать

Корпоративное обучение почти полностью переехало в видеоформат. Онбординг новых сотрудников, курсы по продукту, вебинары для партнёров, записи планёрок — всё это нужно где-то хранить, защищать и давать доступ к десяткам, сотням, а то и тысячам зрителей. Не очень понятно, где разместить весь этот объём знаний и сколько это может стоить.

О том, как устроена экономика профессионального видеохостинга и как бизнес-подразделениям грамотно согласовывать бюджет для его использования, рассказывает Александр Павлычев, сооснователь видеоплатформы Kinescope.

Зачем компании платить за видеохостинг, если есть YouTube и VK Видео



Денис Коннов,
Kinescope

YouTube и VK Видео — хорошие инструменты для публичного контента и маркетингового продвижения. Но как только у вас появляются задачи, которые не предполагают открытого доступа, открытые видеохостинги перестают справляться. Представьте: вы записали обучающий курс для новых менеджеров по продажам.

Загружаете на открытый видеохостинг, ставите скрытую ссылку и думаете, что видео в безопасности. Но любой человек со ссылкой может переслать её дальше, вы это не отследите, а конкуренты смогут подсмотреть методологию, которую в компании выстраивали годами.

Профессиональный видеохостинг закрывает три задачи, с которыми бесплатные платформы не справляются: защита контента, детальная аналитика и отсутствие чужой рекламы и ссылок на сторонние видео. Когда сотрудник смотрит, например, учебный курс на профессиональном видеохостинге, он не увидит рекомендации новостных или развлекательных видео, не будет отвлекаться. Учебный процесс становится более управляемым.

Из чего складывается цена на видеохостинг

Большинство HR-директоров, когда впервые смотрят на счёт за видеохостинг, видят финальную цифру с разным количеством нулей. При этом, за ней скрываются несколько совершенно разных статей расходов. Понимать их по отдельности важно: оптимизировать каждую можно по-своему и, соответственно, экономить бюджет компании.

Главных статей расходов в видеохостинге три: трафик, хранение и транскодирование. Плюс есть ещё дополнительные опции, о них тоже расскажем в конце статьи.

Трафик видео

Трафик — это самая крупная статья расходов. Каждый раз, когда сотрудник или клиент нажимает «Play», видео передаётся от серверов платформы к его устройству. Чем больше просмотров, чем выше качество, тем больше гигабайт уходит и тем больше вы платите.

Ориентиры по объёму данных на час просмотра:

- SD (480p) — около 0,5–0,7 ГБ
- HD (720p) — около 1–1,5 ГБ
- Full HD (1080p) — около 2–3 ГБ
- 4K — до 15 ГБ

Но пользователь не всегда смотрит видео в максимальном качестве. Все профессиональные платформы используют адаптивный стриминг — технологию, которая автоматически подбирает качество под скорость интернета конкретного зрителя. Если сотрудник смотрит курс с мобильного телефона в метро, он получит 480p, а не 1080p. Реальный расход трафика обычно ниже теоретического максимума, это важно учитывать в расчётах.

В стоимость трафика также входит CDN — сеть серверов, распределённых по всей стране или даже миру. Именно CDN обеспечивает быструю загрузку видео независимо от того, где находится зритель: в Москве, Новосибирске или Владивостоке. Если ваш сервер стоит только в Москве, клиенты из Владивостока будут ждать загрузки в несколько раз дольше и, по данным исследований Google, 53% пользователей закроют страницу, если видео не начнётся в течение трёх секунд. Хорошая CDN — это базовое требование, если команда географически распределена.

Как заранее рассчитать бюджет на трафик

Есть простая формула. Нужно знать три числа: сколько часов видео смотрят в месяц, в каком качестве и сколько стоит гигабайт на конкретной платформе.

Возьмём реальный пример: 500 сотрудников, каждый ежемесячно смотрит в среднем 2 часа учебного контента в Full HD. Это 1 000 часов просмотра. Умножаем на 2,5 ГБ — средний расход для Full HD — получаем 2 500 ГБ трафика в месяц.

При стоимости трафика 1,5 рубля за гигабайт — это 3 750 рублей в месяц. На одного сотрудника выходит меньше 8 рублей в месяц.

Именно так и нужно обосновывать бюджет: не «мы тратим X рублей на какой-то хостинг», а «стоимость доставки одного часа учебного контента одному сотруднику составляет Y рублей». Цифры становятся приземлёнными.

Хранение видео

Хранение — статья, которую легко недооценить. Люди думают: «Если у меня 100 видео по часу каждое, значит на хранение уйдёт примерно 100 ГБ». Это не так.

Когда вы загружаете исходный файл, платформа автоматически создаёт несколько версий в разном разрешении — 360p, 480p, 720p, 1080p — чтобы адаптивный стриминг

работал корректно. Плюс делает резервные копии на случай технического сбоя. В итоге один час Full HD-контента в реальном хранилище занимает 6–8 ГБ, а не 1,5 ГБ, как весит исходный файл.

Для небольших библиотек это не критично. Но если компания несколько лет ведёт активное корпоративное обучение и никогда не чистит архив, накопленный объём начинает серьёзно давить на бюджет. Компания продолжает платить за записи трёхлетней давности, которые никто не смотрит.

Практическое правило: раз в квартал просматривайте аналитику просмотров и архивируйте или удаляйте контент, к которому никто не обращается. Хорошие платформы предоставляют такую аналитику в стандартном интерфейсе, не нужно ничего дополнительно настраивать.

Ещё одна статья расходов: транскодирование

Транскодирование — это процесс, который происходит один раз при каждой загрузке видео. Платформа берёт ваш исходный файл и «перепаковывает» его в несколько форматов и разрешений, чтобы видео корректно воспроизводилось на любом устройстве: от смартфона с медленным интернетом до большого монитора в переговорной.

Стоимость рассчитывается за минуту видео и оплачивается один раз. Если перезаливаете тот же файл — платите снова. Поэтому важное правило: загружайте финальную версию видео, а не черновые варианты.

На фоне трафика транскодирование — небольшая статья. Но если вы мигрируете с другой платформы и одновременно загружаете тысячи видео, она может дать ощутимый разовый счёт. Это нужно учитывать при планировании перехода.

Кстати, о миграции видеотеки

Одна из самых популярных видеоплатформ для бизнеса, Vimeo, после 2022 года стала для российских компаний неудобной: платежи усложнились, русскоязычная поддержка исчезла, стоимость хранения выросла. Поэтому мы наблюдали большой рост миграции видеотек.

Технически это не сложно, мы помогаем перенести библиотеку, не теряя метаданные и организационную структуру видеофайлов. А вот организационно будет сложнее. Нужно обновить ссылки в LMS, корпоративных порталах, письмах с доступами. Здесь

важна хорошая документация и интеграции платформы с популярными системами вроде GetCourse, Bizon365 и так далее.

Что касается экономики: Vimeo Enterprise стоил от \$300 в месяц без учёта проблем с оплатой и хранением данных за рубежом. При переходе на российский хостинг компании, как правило, экономят 30–50% бюджета и при этом соответствуют требованиям 152-ФЗ о персональных данных: данные сотрудников, включая видеозаписи с их участием, хранятся на российских серверах.

Если же вы переезжаете с бесплатных видеоплатформ, то процесс миграции технически организован также достаточно просто. Самым сложным остаётся — обосновать бюджет.

Дополнительные расходы на видеохостинги

У каждого профессионального хостинга они отличаются, расскажем о самых популярных.

Первая — защита контента. Базовый уровень — ограничение по домену (видео воспроизводится только на вашем сайте или в вашей LMS) и защита ссылок через пароли. Продвинутый уровень — DRM-шифрование, то есть шифрование по стандартам Widevine и FairPlay. Это тот же стандарт, что использует Netflix: даже если пользователь попытается записать экран, система заблокирует запись на уровне операционной системы.

Некоторые видеохостинги берут за защиту видео отдельную плату. При выборе платформы обязательно уточняйте, входит ли защита в базовую стоимость, какие опции защиты будут вам доступны.

Вторая — аналитика. Стандартный набор открытых видеохостингов: количество просмотров, география, устройства. Для HR-задач этого мало. Нужно понимать, досматривают ли сотрудники курс до конца, на каком моменте уходят, пересматривают ли отдельные фрагменты. Возможно создание тепловых карты вовлечённости и трекинга на уровне конкретного пользователя. Именно по этим данным вы понимаете, работает ли контент: усвоил ли сотрудник материал или просто формально прошёл курс.

Третья — брендинг и интерактивность. Белый лейбл плеера (без логотипа платформы), кастомные цвета — вопрос корпоративной идентичности. Но есть и функциональная составляющая: возможность встраивать в видео кнопки с призывом к действию, формы, главы с навигацией. Для онбординга или продуктовых тренингов это повышает вовлечённость и упрощает навигацию по длинным курсам.

Практические советы по снижению расходов без потери качества

Несколько проверенных приёмов, чтобы снизить давление на бюджет.

Отключите хранение оригиналов видео. Платформа всё равно создаёт оптимизированные версии, исходник нужен только для повторного транскодирования, если в будущем потребуется новый формат. Если такой необходимости нет, хранение оригинала можно отключить. Экономия — двукратная, в зависимости от объёма хранилища.

Калибруйте качество под аудиторию. Если большинство сотрудников смотрит обучение с мобильных устройств, нет смысла платить за трафик 4K. Можно явно ограничить максимум до 1080p или 720p — адаптивный стриминг всё равно подберёт оптимальное качество для каждого пользователя.

Регулярно убирайте неактивный контент. Используйте аналитику: видео, к которым не обращаются больше полугода, можно выгрузить в холодное хранение или удалить. Особенно это актуально для записей вебинаров — их смотрят преимущественно в первые две недели после события.

Договоритесь о прогрессивных тарифах. Большинство платформ снижают цену за гигабайт при росте объёмов. Если вы знаете, что потребление будет расти, имеет смысл обсуждать с платформой долгосрочный контракт заранее.

Как HR-директору обосновать бюджет на видеохостинг

Главная ошибка — представлять видеохостинг как IT-расход. Это расход на учебную инфраструктуру, и считать его нужно в логике стоимости обучения на одного сотрудника.

Сравните: один день очного тренинга для 20 сотрудников с привлечением внешнего тренера стоит от 20 000 до 100 000 рублей. Один и тот же видеокурс можно показать 500 сотрудникам по всей стране за 3 750 рублей трафика в месяц, расчёт мы делали выше. Это инвестиция в масштабируемость обучения.

Второй аргумент — регуляторный риск. Хранение персональных данных сотрудников, включая видеозаписи с их участием, должно соответствовать 152-ФЗ. Штраф за нарушение требований закона и репутационные потери от проверки обойдутся дороже любого тарифа на видеохостинг.

Третий аргумент — операционная устойчивость. Если вы до сих пор используете зарубежный видеохостинг вроде Vimeo с ограниченными возможностями оплаты и поддержки пользователей из России, вы принимаете на себя большой риск за судьбу корпоративной видеотеки.

Как правильно выбирать платформу, если компания только начинает систематизировать корпоративное видео

Шаг 1 — инвентаризация. Посчитайте, сколько часов видео у вас есть сейчас и сколько планируете создавать в год. Оцените среднемесячное количество просмотров или хотя бы число сотрудников, которые будут регулярно смотреть обучающий контент.

Шаг 2 — перевод в гигабайты. Часы просмотра умножайте на коэффициент качества (для Full HD — 2,5 ГБ/ч). Помните, что объём хранилища умножается в 4–8 раз по сравнению с исходником.

Шаг 3 — сравнение тарифов по факту. Не по номинальной цене плана, а по фактической стоимости вашего расчётного объёма. Запрашивайте у платформ конкретный расчёт под ваши параметры.

Шаг 4 — проверка скрытых расходов. Входят ли в тариф DRM, брендинг плеера, интеграции с вашей LMS? Нужна ли доработка со стороны разработчика? Скрытые расходы на интеграцию иногда перекрывают разницу в тарифах между платформами.

Шаг 5 — тестирование на реальном контенте. Большинство платформ предоставляют бесплатный период. Загрузите реальные видео, дайте доступ нескольким сотрудникам и проверьте, как всё работает в ваших конкретных условиях. За две недели тестирования вы поймёте гораздо больше, чем из любого маркетингового материала.

*Денис Коннов, директор по маркетингу Kinescope

Эксклюзивно для



Как выбрать платформу для запуска сайта под свой бизнес

Магазин на Битриксе. Готовое решение или делать с нуля?

Когда предприниматели планируют запуск интернет-магазина, неважно, нового, либо обновление существующего, они так или иначе сталкиваются с дилеммой: взять готовое решение, быстро запуститься и начать работать, либо нанять дизайнера, который нарисует макет, исходя из требований заказчика, а затем внедрить этот дизайн на CMS-систему и запустить проект.

В этой статье рассмотрим, какой вариант и в каком случае стоит выбрать. А также какой подход стоит использовать для того, чтобы принять правильное с точки зрения бизнеса решение. Расскажу о преимуществах и недостатках как готовых решений, так и уникальных дизайнов.

Поскольку Студия WeBrain 12 лет является партнером 1С-Битрикс, а также большинство решений разрабатывает именно на этой CMS (системе управления сайтами), де-факто держим в голове, что речь именно о готовых решениях из Маркетплейса Битрикс, ибо они на мой взгляд являются примером максимальной проработанности и учитывают практически все потенциальные потребности как пользователя, так и владельца. Скажу даже больше: практически во всех проектах, которые мы разрабатывали для малого бизнеса, 60-70% функционала этих готовых решений отключалось за ненадобностью еще на этапе базовой настройки. То есть решения часто перенасыщены функционалом, который требуется уже развитым проектам с большим количеством SKU и перегруженными отделами маркетинга, которые только и успевают, что проводить бесконечные акции, распродажи, тайм-аут промо и прочие маркетинговые активности.



**Евгений
Былинкин**
WeBrain

Разумеется, нужно понимать, что перенасыщенность функционалом — это не недостаток, а заранее заложенный фундамент будущего роста вашего бизнеса. Эти функции в случае успеха проекта непременно вам понадобятся, просто их уже не нужно будет разрабатывать и внедрять — все заранее сделано и работает.

Так вот, что касается разработки интернет-магазинов, есть две мои любимые крайности.

Первая крайность: «давайте возьмем готовое решение и сделаем сами — дешевле и проще».

Дешевле и быстрее — возможно. Проще — вообще не факт. Каждый проект уникален, как и каждое готовое решение. И если ваш подрядчик (либо вы сами) никогда не сталкивался с готовыми решениями, ему будет не так-то просто и быстро разобраться в их архитектуре с нуля, чтобы отсеять лишнее и эффективно применить подходящее.

Например, я являюсь официальным партнером компании INTEC — одного из топовых разработчиков готовых решений на Битрикс. Я разработал на их решениях уже с десяток проектов (раньше пользовался другими решениями), набил руку и сразу понимаю, какие настройки необходимо выполнить, где и что находится внутри этой конкретной архитектуры.

Пример из практики. Как-то один заказчик спросил меня, почему он должен дополнительно оплачивать работу по внедрению, если он и так покупает “готовое решение”. Ответ прост: готовое решение готово не под ваш конкретный бизнес, а с точки зрения разработки основных элементов дизайна и функционала. Это универсальный шаблон, требующий наполнения вашим контентом, кастомизации под ваши бизнес-процессы, часто тонкой настройки модулей и компонентов, чтобы на выходе соответствовать вашим ожиданиям и потребностям.

Вторая крайность: «нам нужен уникальный дизайн, чтобы прям вау».

И здесь очень часто происходит много вещей, влияющих на скорость, бюджет и конечный результат.

Цикл производства такого продукта сложен и состоит из множества этапов, на каждом из которых вы обязательно будете сталкиваться с трудностями, непониманием, “хотелками” собственника, попытками изобрести велосипед, то есть с бесконечным циклом согласования на каждом этапе разработки проекта: брифы, технические задания, прототипы, дизайн-макеты, верстка, функционал.

Думаю, не стоит объяснять, что зачастую выбор такого цикла производства приводит к растягиванию сроков, увеличению бюджета, а также большому количеству потраченных нервных клеток, как со стороны заказчика, так и со стороны исполнителя. А что еще важнее — откладыванию запуска проекта. Пока вы создаете “уникальный” сайт, вы не зарабатываете деньги, а ваш бизнес простаивает.

Словом, обе крайности регулярно заканчиваются одинаково: лишними деньгами и разочарованием.

Каким же образом должна выглядеть вилка выбора

Вы выбираете либо скорость и предсказуемость, либо отстройку и контроль.

Если вы запускаете классический интернет-магазин, я, как стратегический маркетолог, почти всегда за готовое решение.

Потому что этапы запуска классического интернет-магазина уже давно стандартизированы. И чаще всего в этом процессе важнее не креатив, а правильно выстроенные, но вполне себе рутинные цепочки задач.

Обычный набор функционала для магазина: каталог, фильтры, поиск, корзина, оплата, доставка, личный кабинет, скидки, промокоды, статусы заказов, интеграции, SEO-база — всё это давно обкатано. Если на начальном этапе вам достаточно того, что перечислено выше, выбор очевиден.

И вы платите не «за шаблон», а за то, что чужие ошибки уже случились на сотнях других проектов.

Плюс готовое решение отлично подходит, чтобы быстро проверить бизнес-гипотезу: есть ли спрос, сходится ли экономика, не съедает ли логистика всю прибыль с проекта.

На этом этапе уникальный дизайн обычно не спасает.

А вот когда имеет смысл делать с нуля — это почти всегда про ситуацию, где вы выигрываете не «ассортиментом и ценой», а опытом и логикой продукта

Когда покупка не «положил в корзину», а «выбрал из сложного»: конфигуратор, подбор, сравнение сценариев, персональные рекомендации, кастомизация.

Когда бизнес-логика нестандартная: B2B-цены, роли пользователей, КП вместо заказа, индивидуальные условия, куча регионов/складов, сложные правила доставки (и даже такие задачи вполне реализуемы на готовых решениях). Когда вам важно быстро менять сайт под гипотезы — и не жить в ограничениях готовой архитектуры.

Когда бренд держится на ощущениях и интерфейсе (премиум, контент как часть продаж). Тут шаблон часто не помогает, а усредняет. И этот пункт, пожалуй, самый главный. Чаще всего уникальность требуется в проектах, ориентированных на премиальный сегмент.

В качестве примера могу привести сайт практически любой компании, занимающейся арендой автомобилей бизнес- и премиум-класса. В таких бизнесах “премиальность” услуги подается именно через дизайн. И продуктом подобного бизнеса является не только аренда, но и ощущения клиентов от пользования данным сервисом.

Подытожу неочевидной метафорой:

Выбирайте готовое решение, когда нужен надежный «двигатель» и скорость;

Делайте с нуля, когда «форма машины» становится конкурентным преимуществом.

На что стоит обратить внимание при разработке интернет-магазина на готовом решении на Битриксе

В первую очередь, обратите особое внимание на выбор подрядчика.

Он должен как минимум соответствовать следующим критериям:

Иметь официальный статус партнера компании “1С Битрикс”, подтвержденный сертификатом.

Наличие сертификата означает, что компания прошла необходимые тесты и проверки Битрикс, имеет необходимый опыт и квалификацию.

Иметь опыт реализации проектов на конкретном выбранном вами готовом решении.

Как я писал в начале статьи, каждое готовое решение имеет уникальную внутреннюю архитектуру и разбираться в новом для себя решении “с нуля”, значит, тратить в первую очередь время заказчика, которое, как правило, ограничено.

Не обещать выполнить ваш проект по цене только лишь лицензии.

В этом пункте вы сразу отфильтруете невостребованные компании или фрилансеров, которые готовы работать ради работы. Да, партнерская программа Битрикс подразумевает комиссию за продажу лицензий, и это совсем не секрет. Однако, объем работ, который на практике необходимо выполнить для реализации проекта “под ключ” в подавляющем большинстве случаев в денежном выражении значительно превышает размер этой комиссии.

Рекомендация с точки зрения стратегического маркетинга

В конце я бы хотел озвучить алгоритм, который подойдет, пожалуй, большинству новых и существующих компаний, которые запускают собственный интернет-магазин, и который позволит сэкономить максимальное количество времени и бюджета.

Итак, зачастую лучший путь — начать с готового решения: наполнить своим уникальным контентом, выстроить бизнес-процессы, запустить трафик, протестировать не только лидогенерацию, но и процесс обработки заказов вплоть до получения первой прибыли.

Многие либо забывают, либо не думают, что сам по себе интернет-магазин — это всего лишь витрина, а сам бизнес находится вне зоны видимости ваших покупателей. И выстроенные бизнес-процессы гораздо важнее оболочки. Если ваш бизнес работает как часы, бухгалтерия принимает оплаты, склад вовремя отгружает качественную продукцию, то ваши клиенты уже будут вам благодарны и будут возвращаться за повторной покупкой.

Дизайн, красоту и ваши личные хотелки можно дорабатывать и в процессе. Любое готовое решение подлежит постепенной кастомизации без потери качества и без нарушения основных процессов.

Будьте уникальны в первую очередь в предоставлении лучшего сервиса, и очередь из благодарных клиентов обеспечит вам возможность выделяться на фоне конкурентов любыми фишками.

***Евгений Былинкин, руководитель WeBrain**

Как мы продаём gvozd.org

В мире SEO-инструментов появляются десятки новых решений ежемесячно. Наша философия продаж строится на простом принципе: разные аудитории — разные подходы.

Две основные аудитории - две стратегии

Для крупного и среднего бизнеса: разговор на языке прибыли и сокращения издержек.

Когда мы работаем с владельцами компаний и топ-менеджерами, мы говорим не о технических параметрах, а о результатах в деньгах.

Основной канал: персональные презентации для первых лиц. Выход на эти презентации через SEO и контекстную рекламу



Федор
Задков,
gvozd.org

Наша фишка №1: “Финансовый калькулятор ROI” Мы не просто показываем интерфейс. Мы приносим с собой персонализированный расчет:

Сколько ваш бизнес теряет сейчас из-за слабого SEO?

Какой прирост трафика и конверсий даст gvozd.org через 3, 6 и 12 месяцев?

Конкретная сумма дополнительной прибыли в рублях

Наша фишка №2: “Кейс-зеркало” Мы находим компанию в вашей нише (не прямого конкурента, но со схожей бизнес-моделью), которая уже использует gvozd.org, и показываем их результаты. Анонимно, но убедительно.

Что мы делаем на презентации:

Первые 5 минут — говорим только о проблемах бизнеса, а не о функционале

Живая демонстрация на примере сайта компании (с их разрешения)

Сценарий “день с gvozdz.org” — как изменится работа отдела маркетинга

Для маркетологов и SEO-специалистов: разговор на языке экспертов

Этой аудитории не нужны общие фразы. Им нужны конкретные инструменты, которые решают их ежедневные боли.

Основные каналы:

Глубокие публикации в профильных журналах (Cossa, TexTerra, SEOnews)

Вебинары с разбором сложных кейсов

Наша фишка №3: “Тест-драйв на реальном проекте” Не демо-версия, а полноценный доступ к gvozdz.org на 14 дней для работы с одним реальным проектом специалиста. Со всеми функциями, включая экспорт отчетов.

Что мы публикуем в журналах:

Технические исследования — как изменились алгоритмы Яндекса/Google и как gvozdz.org адаптируется

Сравнительные обзоры — честное сравнение с конкурентами (сильные и слабые стороны каждого)

Интервью с пользователями — не отзывы, а подробные истории внедрения

Методические материалы — готовые схемы работы для разных типов проектов

*Денис Коннов, gvozdz.org

Эксклюзивно для



Запрос о том какой именно софт вам нужен – это компас вашей удачи в поиске софта

Автоматизация рекрутмента в небольшом агентстве: как мы нашли рабочую HRM с ИИ и не разорились по дороге Когда управляешь кадровым агентством, быстро понимаешь: твой главный ресурс - это время рекрутеров, а главная статья расходов - их зарплата и софт, который должен эту зарплату окупать.

У нас небольшая команда: пять штатных рекрутеров плюс пул внешних подрядчиков, которых мы подключаем, когда случается высокая загрузка или нужно закрыть 1-3 вакансии, а основные силы уже заняты. Модель гибкая, но она же диктует жесткие требования к инструментам.

Долгое время мы работали на том, что было под рукой: гугл-формы для сбора контактов, доработанный под себя Битрикс24. Но росло количество проектов, росла база кандидатов и клиентов, и стало очевидно: мы теряем эффективность. Информация разрозненна, подрядчики работают вслепую, не видя истории, а на разбор откликов уходят часы, которые могли бы быть потрачены на переговоры. Мы начали искать нормальную HRM-систему. Провели демо с Talantix, СберПодбором, смотрели другие известные платформы. Продукты мощные, спору нет. Но когда начинаешь считать бюджет под нашу модель, картина вырисовывается печальная.



Злата Похалуева,
Бизнес-тренер

Почему мы отсеяли “тяжелый” софт

Первое – стоимость.

Оплата за каждую лицензию.

Для пяти штатных единиц это еще терпимо. Но как только ты добавляешь подрядчиков на проект, сумма умножается. А подрядчики - люди временные.

Платить за них ежемесячно, когда они месяц могут вообще не заходить в систему, просто выбрасывать деньги на ветер. Второе - скрытые платежи. Базовая стоимость - это только входной билет. Дальше начинается: интеграции с работными сайтами за отдельную плату, доступ к API - доплатите. А когда мы начали интересоваться блоками с искусственным интеллектом, выяснилось, что это вообще опция, которая удваивает стоимость подписки. Для небольшого бизнеса такая схема непозволительна. Третье - сложность. Слишком много настроек, статистик, графиков.

Для небольшой компании половина из них просто не нужна. А интеграции нужно отдельно покупать и «прикручивать» к кабинету. Почему мы вообще уперлись в наличие ИИ Где-то год назад мы начали активно использовать ИИ в работе.

Разработали собственного ассистента в чате GPT и делегировали ему рутину: составление продающих объявлений о найме, формирование вопросов для структурированного интервью, написание отзывов о кандидатах на основе записей интервью. Эффект оказался впечатляющим. Мы поняли, что ИИ сильно экономит время рекрутера на рутине. Теперь они могут заниматься действительно интеллектуальной и аналитической деятельностью, успевают проводить больше интервью. Логично, что следующим шагом стал поиск HRM, где этот искусственный интеллект был бы уже вшит в систему, а не работал отдельно. Что мы искали?

К тому моменту у нас сформировался четкий запрос.

Нам нужна была система, которая:

Имеет адекватную цену без скрытых

оплат. Чтобы все интеграции были включены, в том числе блок ИИ. Не требует дополнительных платежей за каждого нового пользователя. Чтобы можно было временно подключать подрядчиков и не терять историю работы над вакансиями. Хранить всю информацию в одном месте.

Помимо блока работы с кандидатами, нам нужна база клиентов. Для кадрового агентства это спасение - держать все базы в одной системе, а не в разных. Имеет встроенный ИИ-функционал, а не опцию за отдельные деньги. Быстро настраивается. Чтобы не тратить недели на внедрение. Хранит данные только на российских серверах. Чтобы не нарушить 152-ФЗ "О персональных данных". Что в итоге получили. Мы нашли решение, которое закрыло все наши запросы. Российская система ReachPoint. Бюджетная, без скрытых платежей, со встроенным ИИ. Рассказываю, как все устроено с точки зрения ежедневной работы. По базовому функционалу - всё стандартно: карточки, воронка, база кандидатов. Но есть несколько вещей, которые реально изменили процессы. - ИИ-фильтр. Позволяет за пару минут разобрать пул откликов на подходящих и не подходящих под вакансию. Есть и обычные фильтры - по городу, программам, языкам, но связка классики и искусственного интеллекта дает совсем другой результат. Рекрутер не тонет в потоке, а сразу видит тех, с кем имеет смысл работать. - HR-ассистент на базе ИИ. Он сам запрашивает у кандидата резюме и задает вопросы для первичного отбора. При этом карточка кандидата с его резюме, ответами и заключением ИИ появляется в системе автоматически. Рекрутеру не нужно ничего догонять, не нужно писать «пришлите резюме». Он заходит в уже подготовленную карточку и принимает решение. - Структура ролей. Удобная и понятная: рекрутер, руководитель, менеджер по работе с клиентами, администратор. Каждый видит ровно то, что нужно для работы, ничего лишнего. - Интеграции с работными сайтами. Опубликованные вакансии на работном сайте автоматически появляются в HRM, отклики на вакансию падают туда же. Ничего не теряется, не нужно ничего экспортировать вручную. - Единая база. Мы наконец-то перестали хранить клиентов в одной системе, а кандидатов

в другой. Вся информация в одном месте. Менеджеры видят историю взаимоотношений с заказчиком, рекрутеры видят историю работы с кандидатами. - Скорость настройки. Внедрили буквально за 20 минут. Без программистов, без внедренцев, без дополнительных оплат. Что в сухом остатке?

Сейчас мы работаем в этой системе и консультируем команду по новым функциям. Первыми тестируем новый функционал - проект продолжает развиваться, и это чувствуется.

Если коротко резюмировать наш путь: мы перестали платить за красивые графики, которые не используем, и за лицензии людей, которые у нас работают временно. Мы нашли систему, где стоимость прозрачна, а встроенный ИИ реально разгружает команду.

ИИ фильтрует отклики, общается с кандидатами на входе, собирает данные. Рекрутеры занимаются тем, что приносит деньги - переговорами и закрытием вакансий. Для бизнеса это чистая математика: меньше рутины - больше закрытых вакансий. Меньше расходов на софт - выше маржинальность. Прозрачные процессы - меньше ошибок и потерь.

*Злата Похалуева, Бизнес-тренер ведущих бизнес-школ по курсу «Управление персоналом», автор и ведущий курса «Профессиональный рекрутер»

Цены на софт для бизнеса в IT: как посчитать эффективность

На рынке IT-компаний затраты на софт давно перестали быть просто статьей расходов. CRM, ERP, системы управления проектами, таск-трекеры, сервисы коммуникаций, аналитика, DevOps-инструменты — все это формирует основу работы компании.

При этом большинство руководителей до сих пор оценивают программное обеспечение только через стоимость лицензий: дорого или дешево. Это ошибка.

Софт нужно оценивать не по цене, а по влиянию на производительность и прибыль.

Стоимость софта — это не только лицензия



Максим Гаёв,
AMI-Sales

Когда бизнес считает расходы на программное обеспечение, он часто смотрит только на стоимость лицензии или подписки. Но в реальности у любого IT-решения всегда есть вторая составляющая — стоимость услуг.

Практически любой софт нужно: - внедрять - настраивать - дорабатывать - интегрировать с другими системами - обучать сотрудников - сопровождать

Именно поэтому в большинстве проектов стоимость услуг составляет не меньшую, а иногда и большую часть бюджета, чем сам софт.

Например, если компания внедряет CRM, она платит не только за лицензии, но и за:

- проектирование процессов - настройку воронок - интеграции с телефонией, почтой, мессенджерами - разработку отчетности - обучение команды

Поэтому корректно считать не только стоимость программного продукта, а полную стоимость владения:

- лицензии
- внедрение
- поддержка
- доработки
- интеграции
- внутренние трудозатраты команды

Только после этого можно объективно оценивать экономику проекта.

Универсальный критерий эффективности — производительность

Если говорить о том, как понять, окупился ли софт, то есть один универсальный критерий — рост производительности.

Любой софт в конечном итоге нужен для того, чтобы сотрудник мог делать больше действий за то же время.

Неважно, о чем идет речь: - CRM — про продажи - ERP — про управление ресурсами - таск-трекеры — про контроль задач - чаты и ВКС — про коммуникации - маркетинговые платформы — про сокращение затрат на привлечение

Любой из этих инструментов должен приводить к одному результату: росту производительности.

Если вчера сотрудник без системы мог выполнить одно действие, а сегодня с помощью софта выполняет десять — значит, производительность выросла.

Именно этот показатель и нужно считать.

Как считать производительность

На практике правильнее всего оценивать эффективность внедрения на горизонте года.

Сначала фиксируются исходные показатели: - сколько задач выполняет сотрудник - сколько заявок обрабатывает - сколько сделок закрывает - сколько времени тратит на типовые действия

После внедрения системы проходит 6–12 месяцев, и показатели сравниваются.

Например: - менеджер обрабатывал 30 заявок в день, стал обрабатывать 50 - проектный менеджер вел 5 проектов одновременно, стал вести 8 - специалист готовил 2 коммерческих предложения в день, стал готовить 10

После этого можно сопоставить рост производительности с затратами на: - лицензии - внедрение - поддержку

И уже дальше считать срок окупаемости: полгода, год или другой период.

Прибыль на сотрудника — ключевая метрика

В IT-компаниях эффективность софта особенно важно считать через прибыль на одного сотрудника.

Прибыль на сотрудника = Общая прибыль / Количество сотрудников

Почему именно эта метрика важна: - IT-компания продает время команды - основная себестоимость — фонд оплаты труда - рост бизнеса без роста штата дает максимальную маржинальность

Если после внедрения софта компания начинает зарабатывать больше тем же количеством людей, значит инвестиция была эффективной.

Облако и коробка: разница в экономике

При выборе решений бизнес часто сравнивает облачные и коробочные системы.

Коробочные решения требуют: - собственной инфраструктуры - серверов - поддержки - обновлений - специалистов внутри компании или внешнего подрядчика

Облачные решения снимают эту нагрузку: - серверная часть остается на стороне вендора - обновления происходят автоматически - вопросы безопасности решает поставщик - масштабирование происходит быстрее

На первый взгляд облачные решения могут казаться дороже за счет подписки, но в реальности они почти всегда дешевле по совокупной стоимости владения.

Особенно это важно для IT-компаний, где время разработчиков и DevOps-команды — дорогой ресурс.

Почему цены на отечественный софт растут не так быстро

Если говорить про российский рынок, то за последние пять лет цены на отечественный софт росли относительно умеренно.

Во многих случаях рост оказался даже ниже инфляции.

Это связано с несколькими причинами.

1. Высокая рентабельность разработчиков

Крупные вендоры изначально строили прибыльный бизнес и могут позволить себе долго удерживать цены.

2. Высокая конкуренция

На российском рынке много разработчиков, особенно в сегменте CRM, ERP, коммуникаций и управления задачами.

Чтобы занимать долю рынка, компании вынуждены держать цены на приемлемом уровне.

3. Подписочная модель

Практически весь софт сейчас продается по подписке.

Даже если компания покупает коробочную систему и устанавливает ее у себя, ей все равно приходится ежегодно платить за: - обновления - техническую поддержку - расширения - сопровождение

Для вендора это означает стабильную базу клиентов и предсказуемый денежный поток.

Из-за этого ему не нужно постоянно увеличивать цены, чтобы покрывать расходы на привлечение новых клиентов.

4. Снижение затрат разработчиков

Зарплаты в IT продолжают расти, но уже не такими темпами, как несколько лет назад.

Дополнительно искусственный интеллект снижает затраты на разработку и поддержку.

С помощью ИИ сегодня можно: - быстрее писать код - быстрее тестировать - автоматизировать поддержку - уменьшать потребность в части персонала

Из-за этого у многих IT-компаний снижается себестоимость разработки и обслуживания продукта.

Импортозамещение и рост стоимости отдельных решений

Есть и исключения.

Если российский продукт приходит на замену иностранному специализированному решению, цены могут быть значительно выше среднерыночных.

Особенно это касается: - узкоспециализированных ERP - инженерного ПО - отраслевых платформ - сложных BI и аналитических решений

Но даже в этом случае российские разработчики обычно ориентируются на стоимость ушедших иностранных систем.

А западный софт традиционно стоил дорого.

Поэтому даже при высокой цене отечественное решение может быть экономически выгодным.

Роль интегратора

Очень важно понимать: сам по себе софт не создает результат.

Результат создает внедрение.

Именно поэтому ключевую роль играет интегратор.

Хороший подрядчик помогает: - зафиксировать исходные метрики - определить, какие показатели нужно улучшить - посчитать потенциальный эффект - выбрать подходящий инструмент - внедрить его под конкретную задачу

Если подрядчик просто «установил систему», но не связал ее с экономикой бизнеса, внедрение почти всегда оказывается неэффективным.

Итог

Софт в IT-компании нужно оценивать не по цене лицензии, а по влиянию на производительность сотрудников.

Любая система должна отвечать на простой вопрос:

Насколько больше действий может выполнять команда после внедрения?

Именно рост производительности и прибыли на сотрудника показывает, окупился ли софт.

При этом считать нужно не только стоимость лицензий, но и затраты на услуги, внедрение, поддержку и доработки.

Только такой подход позволяет объективно оценить экономику любого IT-решения.

*Максим Гаёв, Основатель **AMI-Sales**. Интегратор amoCRM.

Как чашка кофе может спасти компанию от хакера

В рекламе часто можно встретить слоган, что “по цене чешки кофе...” можно что-то купить - чуть ли не автомобиль или накопить на пенсию.

Вот и в случае с информационной безопасностью можно привести похожую аналогию: если вместо того, чтобы пить кофе каждый день по 10 – 15 минут, и тратить это время на совещание или анализ рисков информационной безопасности, то можно сэкономить миллионы рублей и уберечь ключевые активы компании от хакеров и конкурентов.

Давайте подробнее разберёмся, поэтому так происходит и в чем реальная причина.

На самом деле описать все нюансы задачи построения комплексной системы информационной безопасности для компании не представляется возможным в рамках даже нескольких статей - у нас (у “Гладиаторов информационной безопасности”) уже ни одна сотня постов об этом вышла в нашем канале (<https://vk.me/glabit>) и на видеосервисах (например, <https://www.youtube.com/channel/UCVdMxQYsMp2sXqIH5yo2fFw>). Но я попробую сфокусироваться на самом важном.



**Дмитрий
Ушаков,**
«Гладиаторы ИБ»

И здесь важно зафиксировать несколько тезисов, прежде чем мы перейдем к рассмотрению конкретных сценариев:

1) не надо путать реальную безопасность с требованиями соблюдения нормативных требований, которые обычно трансформируются в формальное соответствие “на бумаге” - так называемую “бумажная безопасность”;

2) это не отменяет того факта, что требования нормативных документов важны, их надо соблюдать, поскольку в своей основе они подсвечивают важные аспекты защиты данных или активов компании;

3) информационная безопасность никогда не была и не будет бизнес-процессом, который генерирует для компании выручку. Это всегда “защитная”, а не “атакующая” функция - то есть через задачи безопасности можно контролировать ущерб, риски, снижать вероятности, но на этом невозможно заработать – эффекты раскрываются только в случае кризиса (когда реализовался какой-то инцидент безопасности - можно назвать его “черным лебедем”. Отличие от “черных лебедей” в бизнесе в том, что в случае инцидентов информационной безопасности мы можем сами управлять вероятностями и влиять на “скорость” возникновения этих инцидентов)

4)

**невозможно прийти в состояние
“защищенности” раз и навсегда —
это всегда длительный процесс,
которому нужно уделять внимание
и за который должен быть
ответственный.**

Таким образом, мы приходим к концепции, что “информационная безопасность” - это одна из зон ответственности компании, где должен быть либо свой собственный руководитель, либо наемный профессиональный аутсорсер со стороны.

Сложности с закрытием этой зоны ответственности обычно связаны с тем, что здесь тяжело выделить какие-то ключевые операционные показатели (KPI), по которым можно оценивать качество реализации данной функции.

Например, количество обнаруженных вирусов: когда их много – это хорошо или всё-таки плохо?

С одной стороны, раз нашли – это хорошо, значит, система безопасности работает. Но если посмотреть на это с другой стороны, то если вирусы появляются, значит в самой сути нашей системы безопасности есть пробоина, через которую вирусы попадают в сеть. Значит, это плохо

. А нулевое число обнаруженных вирусов – это хорошо, значит, защита работает? Но это также может означать, что у нашей системы защиты и детектирующих функций нет, они просто ничего “не видят”!

Как видим, здесь нет однозначного ответа - он будет зависеть от целей и задач, которые мы ставим перед “защитой от хакера”, ведь средства или регламенты защиты - это всего лишь инструменты. Как и с чашкой кофе или молотком - их надо уметь применять.

Так как же всё-таки, успевать и кофе пить, и выстраивать систему информационной безопасности для бизнеса, на что обращать внимание. Давайте разберём несколько примеров инцидентов.

Сценарий №1: вирус-шифровальщик уничтожил базу 1С компании

Типичный случай, с которым зачастую обращаются компании с просьбой помочь даже не в расследовании, а в восстановлении после инцидента. 1С - это одна из ключевых систем любой организации, в которой находится весь хозяйственный учёт предприятия. Из-за потери этой системы можно лишиться и первичной документации и, как следствие, получить штрафы от налоговой, можно потерять информацию о текущих сделках, поставщиках, логистических цепочках, особенностях и структуре сделок. Поэтому когда вирус шифровальщик через компьютер бухгалтера находит сервер 1С и уничтожает на нём информацию – это катастрофа не только для отдела бухгалтерии, но и для компании в целом.

Ситуация обычно усугубляется тем, что бухгалтерия не является квалифицированным пользователем компьютеров, слабо разбираются в технологиях, недостаточно бдительна к

современным Интернет угрозам (например, очень слабо разбирается в техниках социальной инженерии, которую активно применяют злоумышленники для заражения компьютеров). А ещё бухгалтеры активно и без должной осмотрительности пользуются внешними ИТ-подрядчиками, которые помогают им решить вопросы настройки рабочих мест, работоспособности систем, интеграции разных модулей между собой - нередко возникает ситуация, когда бухгалтер без опасений разрешают прямое удалённое подключение к своему компьютеру с функцией полного контроля (что категорически нельзя делать из соображений безопасности - для этого есть другие, более безопасные инструменты)!

Одним словом, когда база данных 1С оказалась уничтожена (шифрование без возможности восстановления – равносильно уничтожению), единственный способ привести систему работоспособное состояние - это восстановить её с нуля. Для этого обычно помогает резервное копирование. Но эти резервные копии нужно делать

а) регулярно

б) заблаговременно

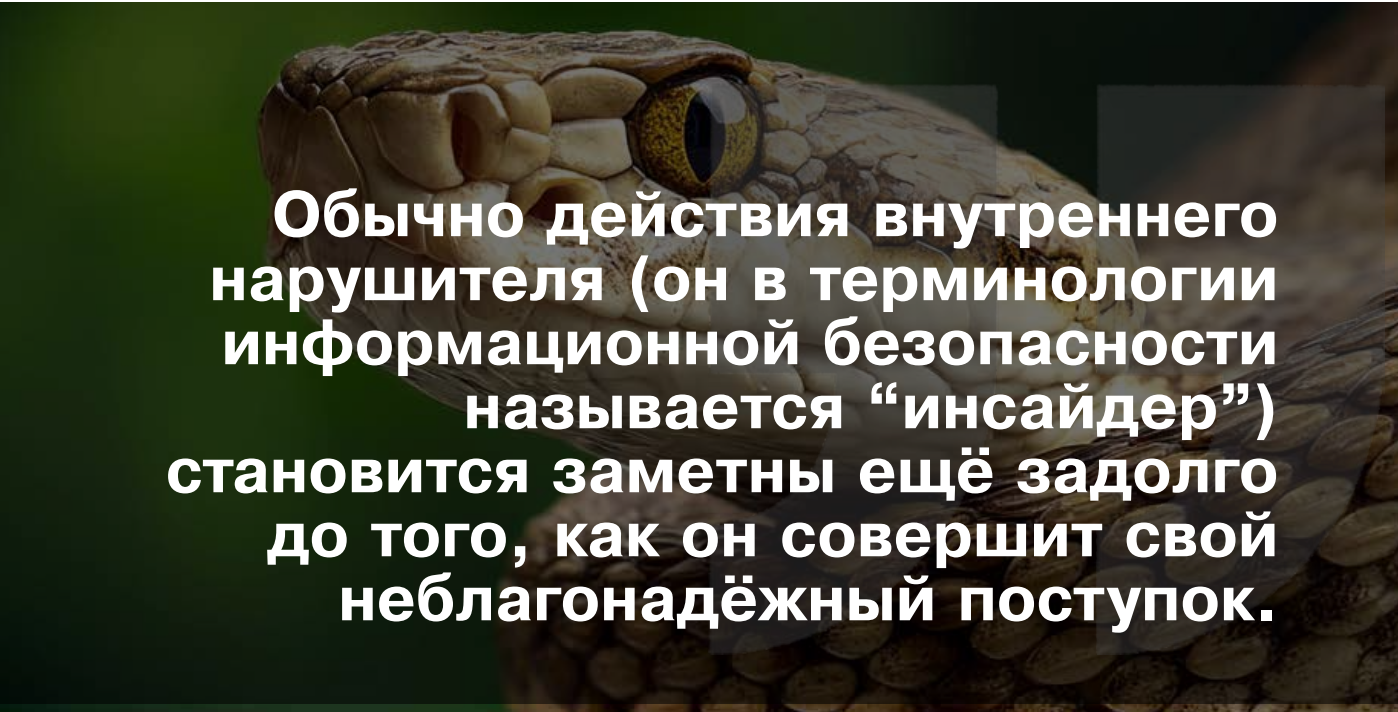
в) (и это также зачастую упускают) нужно тестировать возможность восстановления с созданной резервной копии.

Таким образом, если потратить всего полчаса – час на автоматизацию создание резервных копий и по 15-30 минут в неделю на контроль выполнения этой задачи, добавив сюда примерно 1 час в месяц на проверку работоспособности резервной копии, то можно (при определенных условиях) гарантировать, что организация легко восстановится после атаки даже самого современного вируса шифровальщика.

Тогда в этом примере у нас появляется совершенно конкретная метрика, по которой мы можем отслеживать эффективность применения такого средства защиты, как резервная копия: это будет факт наличие или отсутствия (1 или 0) резервной копии по итогу недели. С этой задачей может справиться даже любой более-менее грамотный помощник – ассистент. Но ему нужно поставить эту задачу, а также регулярно проводить с ним совещание по данной зоне ответственности.

Сценарий №2: сотрудник скопировал секреты производства компании и продал конкуренту.

Другой не самый типовой, но “болезненный” случай, когда информационной безопасности может спасти миллионы нервных клеток и рублей выручки.

A close-up photograph of a snake's head, showing its scales and eyes. The snake is looking towards the right. The image is used as a background for a text overlay.

Обычно действия внутреннего нарушителя (он в терминологии информационной безопасности называется “инсайдер”) становится заметны ещё задолго до того, как он совершит свой неблагоприятный поступок.

А именно, он в частном порядке переписывается с конкурентами, которые пытаются его подкупить, не стесняются использовать для этого даже корпоративные устройства (телефон или ноутбук), а сама переписка ведётся в мессенджерах или личной электронной почте.

По статистике обычно это планируется за несколько недель или даже месяцев – поэтому у подготовленной службы информационной безопасности есть достаточно времени, чтобы обнаружить и предотвратить нарушение.

Функции контроля сотрудников могут затрудняться из-за архитектуры работы с конфиденциальной информацией компании – например, большинство сотрудников подключаются удалённо через VPN. Но при грамотно организованной системе удалённого доступа это не является проблемой, так как сам контроль реализуется на терминальных серверах, к которым подключаются и через которые работают сотрудники. Поэтому установка агентов мониторинга происходит не на конечных рабочих местах, а на точках концентрации информационных потоков.

Более того, чтобы иметь возможность отслеживать подготовку операций и не “спугнуть” инсайдера используются не блокирующие, а “наблюдающие” функции средств защиты -

это означает, что коммуникация инсайдера и конкурента разрешается (до определённых заданных пределов), но при этом все действия подробно регистрируются.

Таким образом убивается сразу два зайца: и функции мониторинга сохраняются, и нарушитель не занят активным заметанием следов, что упрощает его обнаружение.

В данном сценарии точки контроля будут уже совершенно другие, равно как и квалификация сотрудника, которому будет поручена эта зона ответственности.

Так, из операционных показателей можно выделить число ключевых слов для мониторинга, количество каналов перехвата информации, сформированный еженедельный отчёт (с расшифровкой для руководства).

Квалификация специалиста будет уже требовать аналитических способностей, а также частичные знания информационной инфраструктуры предприятия, чтобы иметь возможность составить как паттерны конфиденциальной информации, за который нужно будет следить, так и понимание точек возможной утечки информации (перехвата трафика).

Для того чтоб контролировать работу такого специалиста, необходимо раз в неделю получать от него осмысленный отчёт и разбирать на получасовом совещании – как раз хватит, чтобы заодно выпить и чашку кофе.

Сценарий №3: организация получает штраф за неправомерную обработку персональных данных на своем сайте

Этот сценарий ещё более популярен в последнее время из-за того, что регулирующие органы (в частности Роскомнадзор) начали проверять соответствие требованиям закона 152-ФЗ по набору формальных признаков, случайным образом сканируя сайты компании в Интернет.

Это можно сделать даже не приходя в офис, а просто проверив сайт и выделив на нём набор ключевых метрик: например, передача данных сторонним сервисам аналитики, таким как Google Analytics (это считается трансграничной передачей данных и по умолчанию запрещено), отсутствие политики конфиденциальности на сайте, доступной к изучению, отсутствие явно выражаемого пользователем согласия на сборы и обработку своих персональных данных под формами сбора лидов, которые есть на сайте.

Кажется, что это пустяки, но в данном случае сам дух закона преследует важную функцию – упорядочивания сбора конфиденциальной информации и приведения в порядок бизнес процессов организации. В частности нет смысла собирать какую-то информацию просто для того, чтобы она была – поэтому всегда должна быть обоснованность сбора персональных данных.

Более того, клиентский сервис зачастую зависит от качества обслуживания клиентов, а также от их обратной связи - поэтому, бизнес должен реагировать на их жалобы (в частности просьбы удалить свои персональные данные и больше “не звонить”) - об этом закон и “печётся” и, таким образом, помогает предпринимателем упорядочить (и даже поднять качество) бизнес процессов.

Чтобы в данной ситуации отслеживать показатели “безопасности” необходимо составить чеклист для контроля сайта - в принципе, это может сделать и свой собственный специалист ИТ-шник в течение нескольких дней (или недели).

А ключевой метрикой можно поставить сумму взысканий (штрафов, включая жалобы от конечных пользователей) - и на этом фокусировать ответственного сотрудника.

Еженедельные совещание можно проводить по изменениям законодательства в области контроля персональных данных и числовой метрике равной количеству жалоб.

Как мы видим, если подойти к вопросу информационной безопасности с управленческого подхода, то все становится достаточно логично и понятно, а уж тем более легко поддается контролю даже “не-ИБшнику” - главное не забывать не только пить кофе, но и уделять фокус задачам безопасности.

Вместо заключения – что делать?

Завершая эту короткую статью, приведём перечень того, что необходимо сделать, чтобы подобных инцидентов информационной безопасности в компании не происходило:

1) необходимо выделить перечень ключевых бизнес процессов для своей компании – руководителей про них точно знают, просто могут не формализовать в виде списка/диаграммы/блок-схемы

2) определить набор так называемых “недопустимых событий” - сценариев, при которых компания терпит прямой или косвенный ущерб (обычно он меряется в совершенно

конкретной сумме денег - мы можем помочь оценить этот ущерб с помощью универсального калькулятора, для этого обратитесь на info@glabit.ru)

3) сформировать набор компенсирующих мер, чтобы снизить потенциальный ущерб – так мы видели выше, это может быть как использование средств защиты (программы или программно-аппаратные комплексы – например, антивирусы), так и выстроенные своими же специалистами процессы (например, резервное копирование или регулярное обновление антивируса)

4) расставить точки контроля для регулярной проверки выполнения защитных функций (кстати, такой точкой контроля может быть и внешний независимый аудит безопасности компанией, специализирующийся на защите информации – это называется “тест на проникновение” - обращайтесь на info@glabit.ru, поможем!)

Если у вас ещё остались вопросы или сложности с оценка бизнес процессов или необходимостью их выстраивания, построением системы защиты – вы всегда можете обратиться к нам, “Гладиаторам ИБ”, заполнив форму на сайте - <https://glabit.ru/contacts>

Ну а теперь пойдёмте пить кофе - ведь, как реализовать защиту, мы уже разобрались – появилось ощущение уверенности, контроля на кончиках пальцев, то есть возможность отдохнуть!

*Дмитрий Ушаков, генеральный директор «Гладиаторы ИБ»

Эксклюзивно для **ITРЕВЬЮ**

**ВМЕСТЕ С ITREVIEW ВЫ ПОЛУЧАЕТЕ В ПОДАРОК
ОТ ИЗДАТЕЛЯ ЖУРНАЛЫ В ЭЛ ВЕРСИИ:**



ПОЧТА 7447273@BK.RU

IT-аутсорсинг-2026: кто на коне, а кто ушел в вайб-кодинг?

Рынок больше не единый. Пока одни игроки бьются за демпинговые контракты, другие растут на сложной архитектуре и кибербезопасности. А самые простые задачи заказчики теперь решают с помощью инструментов искусственного интеллекта, не привлекая подрядчиков. Разбираю, какие виды аутсорсинга в плюсе, какие теряют позиции, и кто такие «закрытые» подрядчики.

Рынок вырос, но подход к расходам изменился

Согласно данным TAdviser, российский рынок ИТ-услуг и аутсорсинга в 2024 году увеличился на 25%, достигнув 815 миллиардов рублей. В 2025 году рост составил ещё 15%, превысив 937 миллиардов. Цифры внушительные. Однако динамика замедляется: после 25–30% в 2023–2024 годах сейчас мы видим 10–15%.

Причина в изменении экономической модели. Высокая ключевая ставка сделала заёмные средства дорогими, а инвестиции — избирательными. Компании больше не запускают инициативы «на будущее» — им требуется быстрая окупаемость. Крупные проекты откладываются, фокус смещается на операционную эффективность. Рынок труда также претерпел изменения. Дефицит кадров, характерный для предыдущих лет, сменился более взвешенным подходом: ИТ-бюджеты на 2026 год сокращаются в среднем на 10–15%. Организации активнее переходят к модели привлечения внешних подрядчиков вместо содержания избыточного штата. Содержать людей в простое — дорого, и это понимают все.



**Елена
Назарова,**
ItFox

Что это означает для рынка аутсорсинга? Деньги в ИТ есть, но подход к их расходованию стал иным. Заказчик требует предсказуемого результата и скорости. А скорость сегодня напрямую зависит от того, использует ли подрядчик инструменты искусственного интеллекта. Если нет — он работает медленнее, а значит, его услуги дороже для клиента. И клиент это видит.

Модели, теряющие позиции

Рынок больше не ориентирован на «просто написание кода». Ценность сместилась от количества написанных строк в сторону экспертизы, ответственности и понимания бизнес-контекста. Особенно заметно это на трёх форматах, которые ещё недавно составляли основу бизнеса многих компаний.

Модель «продажи специалистов». Простая аренда разработчиков, особенно среднего уровня. Предложение «команда из десяти миддлов, но быстро обучаемых» больше не вызывает интереса. Заказчики устали от длительного введения в проект, ошибок, которые ложатся на их бюджет, и обещаний «сейчас разберёмся». Специалисты ниже уровня синьор перестали быть товарным продуктом. Выращивать их внутри компании — необходимо, но продавать как основной актив — больше не работает. Рынок не готов оплачивать обучение чужих сотрудников напрямую.

Исполнители, работающие строго по техническому заданию. Раньше такая модель работала безотказно: заказчик формулировал требования, подрядчик писал код. Заказчик мог позволить себе экспериментировать, уточнять требования в процессе, искать оптимальные решения вместе с подрядчиком. Сегодня экономика изменилась. Бюджеты ограничены, и тратить лишние средства на «давайте попробуем так, а потом переделаем» никто не готов. Клиенту нужен не просто код, соответствующий ТЗ, а решение, которое будет эффективно работать в его бизнес-контексте. Он ждёт от подрядчика чётких сроков и предсказуемого результата — без права на долгие уточнения и итеративный поиск. Именно поэтому спрос на «чистые руки» без понимания цели падает: такой подход не даёт клиенту главного — экономии, скорости и уверенности в результате.

Подрядчики, не использующие искусственный интеллект в процессах. Скорость разработки сегодня вышла на первый план. Заказчики ждут результатов быстрее, чем раньше, и не готовы ждать, пока подрядчик сделает работу вручную. Выполнение простых, типовых задач без современных инструментов становится неконкурентоспособным. Этому есть две причины. Первая — рост производительности благодаря искусственному интеллекту у тех, кто его внедрил. Вторая — использование средств искусственного

интеллекта самими заказчиками. Небольшие продукты — лендинги, простые сервисы, базовые интеграции — клиенты всё чаще делают самостоятельно с помощью доступных инструментов. Это быстрее и дешевле, чем привлекать подрядчика, который работает по старинке.

Растущие направления: кто укрепляет позиции

Пока одни форматы теряют рынок, другие показывают устойчивый рост — там, где ценность определяется не количеством задействованных специалистов, а экспертизой и ответственностью.

Аутсорсинг кибербезопасности. 2025 году больше 70% компаний увеличили вложения в передачу функций безопасности внешним провайдерам. Рынок SOC-аутсорсинга вырос на 35%. Причина — дефицит кадров в ИБ превысил 55 тысяч человек, а угрозы становятся сложнее. Заказчики перестали выбирать «продукты» — теперь им нужна функциональность. Больше половины новых контрактов заключаются на полное или частичное управление кибербезопасностью. Особенно вырос спрос на сервисы на базе ИИ: проактивная киберразведка, автоматизированный анализ инцидентов — здесь рост достиг 40%. Заказчики из финансового и промышленного секторов всё чаще передают на аутсорсинг и мониторинг инцидентов, и узкие направления вроде расследования инцидентов. Это позволяет им не отвлекаться на операционную рутину и не пытаться закрыть дефицит редких экспертов.

Рынок окончательно перешёл из «техподдержки» в стратегическую плоскость.

Аутсорсинг сложной архитектуры и импортозамещения. Эйфория 2022–2023 годов («срочно заменить всё, хоть как-нибудь») закончилась. Сегодня заказчики приходят с другими вопросами: как это решение будет поддерживаться через год? Сколько будет стоить владение? Что произойдёт, если ключевые специалисты покинут проект? Им нужны партнёры, которые понимают контекст, а не просто готовы написать код. Спрос сместился в сторону архитекторов, а не программистов, выполняющих точечные задачи.

Управляемый результат (фиксированные сроки — фиксированная цена). Клиенту продаётся не команда, а решение бизнес-задачи. Подрядчик берёт на себя ответственность за то, что система принесёт экономию или будет работать так, как нужно заказчику. Бизнесу нужен не код, а изменения: управляемые сроки, понятная экономика, прогнозируемый результат.

Внедрение прикладного искусственного интеллекта. Период экспериментов «давайте попробуем» остался в прошлом. Работают только те проекты, где заранее понятно, что именно даёт экономию — деньги, время или трудозатраты. Спрос формируется вокруг задач аналитики, автоматизации процессов, поддержки пользователей. Искусственный интеллект рассматривается как инструмент для повышения эффективности, а не как самоцель.

Искусственный интеллект как новая норма

В АЙТИФОКС мы системно внедряем искусственный интеллект в процессы разработки. Генерация кода, автотесты, анализ требований, документирование — везде, где это ускоряет работу. Но с обязательным контролем со стороны человека. Без этого нельзя: качество и безопасность остаются приоритетом. Сегодня наличие искусственного интеллекта в процессах подрядчика — это не конкурентное преимущество, а обязательное условие для работы на рынке. Если компания не использует современные инструменты, она работает медленнее и, следовательно, дороже. Клиенты быстро это просчитывают.

«Закрытые» сегменты аутсорсинга

Существуют сегменты, которые остаются в тени публичных тендеров и маркетинговой активности. Они растут, но о них не принято говорить открыто.

Первый — аутсорсинг для государственных компаний и корпораций. Высокие требования к безопасности и лицензированию создают барьеры входа. И как следствие — высокую маржинальность. Это закрытая зона, доступ в которую возможен только при наличии соответствующей аккредитации и долгосрочной репутации.

Второй — аутсорсинг для непубличных компаний из секторов, находящихся на подъёме: оборонно-промышленный комплекс, фармацевтика, высокотехнологичное производство. В этих отраслях иной подход к финансированию и срокам. Длинные бюджеты, сложные технические задачи, высокий уровень ответственности. Такие заказчики не выбирают подрядчика по прайс-листу — они ищут партнёров, способных работать в жёстких условиях и брать на себя риски.

Что важно учитывать заказчикам и руководителям ИТ-направлений

При выборе подрядчика недостаточно оценивать стоимость часа работы. Необходимо выяснить, как компания использует искусственный интеллект в своих процессах. Если подрядчик не может продемонстрировать, как современные инструменты

повышают его производительность, заказчик будет платить за «ручной труд» по цене автоматизированного.

Руководителям, в чьём ведении находится внутренняя ИТ-разработка, стоит оценить, насколько их команды используют искусственный интеллект. Те, кто этого не делает, рискуют потерять конкурентоспособность даже внутри собственной компании. Когда цена ошибки высока, а скорость вывода продуктов на рынок критична, отказ от современных инструментов — неоправданная роскошь.

Подводя итог: рынок аутсорсинга не умер — он пересобрался. Исчезли модели, которые работали на «продаже рук» и выполнении простых задач по ТЗ. На их место пришли направления, где ценность определяется экспертизой, умением управлять неопределенностью и ответственностью за результат.

Кибербезопасность уверенно вышла в лидеры — компании всё чаще передают её на аутсорсинг, потому что держать своих экспертов дорого, а угроз становится только больше. Сложная архитектура и импортозамещение тоже растут: заказчикам нужны не те, кто напишет код, а те, кто спроектирует систему, которая будет жить годами. Управляемый результат и внедрение прикладного ИИ — ещё два направления, где спрос устойчив, потому что там понятна экономика и есть измеримый эффект.

Искусственный интеллект стал базовой технологией, которая меняет экономику разработки. Те, кто его не использует, работают медленнее и дороже — и клиенты это видят.

В 2026 году на ИТ-аутсорсинге востребованы те, кто способен быстро и качественно создавать сложные продукты, кто внедряет новые инструменты осмысленно, а не ради хайпа, и кто берёт на себя ответственность за результат. Простые же задачи, как и прежде, будут уходить туда, где их можно решить быстрее и дешевле — сегодня это средства искусственного интеллекта, и этот тренд будет только усиливаться.

*Елена Назарова, CEO ItFox

Эксклюзивно для



Кейсы аудитов кибербезопасности различных компаний

Аудиты кибербезопасности — критически важный процесс для любой компании. Он помогает выявить многие уязвимости до того, как ими воспользуются злоумышленники. Рассмотрим типовые кейсы, в которых аудит обнаружил серьёзные проблемы с защитой данных.

Кейс аудита информационной безопасности ИБ: аудит с использованием OSINT и раскрытием скрытых угроз

OSINT (Open Source Intelligence, разведка по открытым источникам) — метод сбора данных из общедоступных ресурсов для анализа защищённости компаний и организаций. Рассмотрим кейс аудита, в котором OSINT помог выявить критические уязвимости до их эксплуатации злоумышленниками.

Цель и задачи аудита информационной безопасности

Компания заказала аудит для оценки внешнего периметра безопасности. Цель выявить с позиции потенциального злоумышленника:

- 🔍 утечки конфиденциальной информации;
- 🔍 открытые ресурсы с недостаточным уровнем защиты;
- 🔍 данные, которые могут быть использованы для целевых атак.



**Дмитрий
Тулупов**

консультант по
Кибербезопасности и ИИ

Методы OSINT, применённые в ходе аудита

Были использованы следующие инструменты и источники:

1.Поисковые системы с продвинутыми операторами поиска для нахождения:

- Открытых документов с метаданными;
- Веб-интерфейсов административных панелей.

2.Базы данных утечек — проверка корпоративных email-адресов на предмет их компрометации.

3.Социальные сети и форумы — анализ профилей сотрудников для выявления:

- Публикаций с фото офисного оборудования;
- Упоминаний внутренних систем и сервисов.

4.Сервисы сканирования инфраструктуры — поиск открытых портов и сервисов, привязанных к IP-адресам компании.

5.Анализ DNS-записей — выявление поддоменов, которые могли быть забыты при реорганизации сети.

6.Архивы веб-страниц (Wayback Machine) — изучение старых версий сайта на наличие ссылок на тестовые среды.

В результате проведенного аудита информационной безопасности обнаружены:

- Утечка внутренних документов: через поисковые системы были найдены различные файлы с планами сетевой инфраструктуры и списками сотрудников.
- Открытые административные панели: веб-интерфейсы CRM и ERP-систем с доступом извне, некоторые — без аутентификации.
- Компрометированные учётные данные: email-адреса сотрудников присутствовали в базах данных утечек; пароли к ним возможно использовались повторно и для других сервисов.

- Публичные репозитории: в открытом доступе были найдены фрагменты исходного кода с прописанными тестовыми учётными данными.
- Аккаунты сотрудников в соцсетях: были найдены публикации с офисными фото рабочих мест и ноутбуков, где были видны пароли, записанные на стикерах.

Кейс внутреннего аудита кибербезопасности: слабые пароли и открытый Wi-Fi как угроза для IT-компании

Выявленные уязвимости

В ходе проведения тестирования информационной безопасности ИБ были обнаружены несколько типов проблем с парольной защитой:

- Стандартные пароли — комбинации, которые часто используются «по умолчанию» и легко подбираются (Например, admin/admin, user/1234 и другие).
- Простые пароли — короткие последовательности или общеупотребимые слова, поддающиеся брутфорс-атакам (Например, 123456, qwerty, password и другие).
- Пароли по умолчанию — заводские настройки, которые не были изменены после развёртывания оборудования или ПО.

Такие пароли использовались на различных ресурсах компании — от учётных записей сотрудников до административных интерфейсов сетевого оборудования. Это создавало прямую угрозу несанкционированного доступа.

Но наиболее критичной оказалась другая уязвимость: гостевой Wi-Fi, который давал доступ ко внутренней сети компании. Любой пользователь, подключившийся к этой сети, получал доступ к:

- корпоративным проектам;
- IP-телефонам (что потенциально позволяет перехватывать звонки);
- принтерам и МФУ (через которые потенциально можно получить конфиденциальные документы);

- другим сетевым устройствам и сервисам.

Аудит кибербезопасности веб-ресурсов медицинской организации: утечка данных через открытые архивы

В ходе проведенного аудита информационной безопасности были выявлены следующие проблемы:

- Веб-ресурсы, доступные извне без аутентификации. Отдельные сервисы и административные панели были открыты в публичном доступе — их можно было найти через поисковые системы или с помощью сканеров уязвимостей.
- Архивные документы отдела кадров в открытом доступе. На серверах и веб-порталах хранились множество архивов документов: сканы паспортных данных, сведения о зарплатах и премиях.
- Устаревшие резервные копии. Забытые бэкапы данных содержали актуальные на момент создания записи, включая контакты пациентов и сведения об оказанных им услугах.

Доступ к этим ресурсам мог получить любой пользователь интернета — достаточно было знать URL или подобрать путь к папке.

Аудит информационной безопасности промышленного предприятия: как расширение периметра выявило скрытые уязвимости

Исходные условия и ограничения

Заказчик предоставил ограниченный периметр для исследования — несколько тестовых серверов и рабочих станций, которые, на первый взгляд, не содержали значимых уязвимостей. Вероятно, этот набор ресурсов был предложен системными администраторами с целью минимизировать риск обнаружения серьезных проблем в основной инфраструктуре.

На начальном этапе проверки:

- не было выявлено критических уязвимостей;

- Базовые настройки безопасности соответствовали минимальным требованиям;
- Система выглядела относительно защищённой.

Расширение периметра и обнаруженные проблемы

После согласования с руководством предприятия периметр сканирования был расширен на смежные сегменты сети. Результаты оказались тревожными: были выявлены многочисленные уязвимости на критически важных объектах:

- Устаревшее ПО на серверах и АСУ ТП. Обнаружены системы с незакрытыми уязвимостями, для которых давно были выпущены патчи, но они не установлены.
- Компьютеры с отключёнными средствами защиты. На ряде рабочих станций были деактивированы фаерволы и средства защиты, что делало их лёгкой мишенью для атак.
- Сетевое оборудование с паролями по умолчанию. Роутеры, коммутаторы и промышленные контроллеры использовали заводские комбинации (admin/admin, guest/guest), доступные в открытых источниках.
- Открытые порты и сервисы. Множество устройств имели активные сетевые службы (SSH, RDP, SMB), доступные извне без должной аутентификации.
- Отсутствие сегментации сети. Производственные сегменты не были изолированы от офисных, что позволяло потенциальному злоумышленнику перемещаться между зонами.
- Незащищённые резервные копии. Бэкапы данных хранились на общедоступных сетевых дисках без шифрования.

Найденные уязвимости создавали серьёзные угрозы безопасности:

- Остановка производственных линий из-за кибератаки на АСУ ТП;
- Утечка коммерческой информации и технической документации;

- компрометация учётных записей администраторов;
- внедрение вредоносного ПО (в т.ч. шифровальщиков — ransomware);
- нарушение работы критически важной инфраструктуры.

Последствия и риски кибербезопасности для различных компаний

Подобные выше уязвимости могли привести к очень серьёзным последствиям:

- утечке конфиденциальной информации;
- компрометации персональных данных;
- несанкционированному управлению корпоративными устройствами;
- нарушению многих бизнес-процессов;
- внедрению вредоносного ПО во внутреннюю инфраструктуру компаний;
- финансовым потерям и репутационному ущербу.

Расчёт потенциального ущерба (по методике OCTAVE):

- прямой ущерб — до 5 млн руб. (восстановление систем, штрафы);
- косвенный ущерб — до 15 млн руб. (потеря контрактов, репутационные риски).

*Дмитрий Тулупов, консультант по Кибербезопасности и ИИ

Эксклюзивно для



Цены на софт для бизнеса в ИТ – как посчитать эффективность

Плохой софт может стоить дешево, но при этом оставлять компанию в том же хаосе, только уже с красивым интерфейсом.

У бизнеса есть старая и очень дорогая привычка - выбирать софт по цене лицензии, красивому списку функций и обещаниям подрядчика. Потом проходит полгода. CRM стоит. ERP работает. Отчеты строятся. Подрядчик сдал проект. А собственник задает неприятный вопрос: где деньги?

Самая частая ошибка здесь в том, что эффективность софта пытаются считать там, где ее удобнее считать, а не там, где она действительно рождается. Смотрят на стоимость лицензии, внедрения и поддержки.

Иногда смотрят на скорость работы внутри одного отдела. Но бизнес не живет внутри отдела. Он живет в сквозной цепочке: от первого обращения клиента до оплаты, от заявки на закупку до прихода товара, от планирования до выпуска продукции. И если новое решение не убирает потери на этих переходах, оно может быть хоть дешевым, хоть модным, но для компании оно останется дорогим. Почему дешевый софт часто обходится дороже дорогого? Предпринимателю обычно продают продукт в логике “что умеет система”.



**Александр
Ожерельев**
NeoGraph.tech

Но реальный вопрос должен звучать иначе: какую потерю в процессе система снимает и сколько эта потеря стоит компании в месяц. Допустим, у бизнеса уже есть CRM. Менеджер заводит заказ быстро, карточка красивая, отчеты есть. Но дальше данные едут на склад через Excel, логистика оповещает в чате, бухгалтерия перебивает документы вручную, а клиенту статус заказа сообщают по памяти. Формально софт внедрен. По факту скорость процесса не выросла, ошибок меньше не стало, руководитель все так же дергает людей по телефону, а прибыль продолжает утекать в паузах между отделами. Именно поэтому я почти всегда предлагаю считать эффективность не от цены продукта, а от четырех вещей

1. Сколько времени уходит на стыки между функциями
2. Сколько ручных действий и повторного ввода данных остается после внедрения.
3. Сколько ошибок, просрочек и потерянных заявок система реально убирает.
4. Насколько быстрее руководитель получает управляемость, а клиент - результат.

Это звучит проще, чем классический TCO (совокупная стоимость владения) и ROI (окупаемость инвестиций), но на практике дает более честную картину. Где на самом деле теряются деньги? В живом бизнесе деньги редко сгорают внутри одной кнопки. Они уходят в ожидание, вручные пересылки, в потерянные уведомления и в отсутствие общего статуса.

Мы в своей практике E2E-диагностики видим устойчивый паттерн: самая дорогая часть процесса - не работа как таковая, а передача работы дальше. Менеджер оформил заказ за 12 минут. Хорошо. Но заказ ушел на склад через полтора часа. Склад собрал его вовремя, но логистика узнала о готовности еще через два часа.

Документы дошли до бухгалтерии в другом формате. Клиенту никто не написал. В итоге компания уверена, что у нее проблема со складом, хотя реальный узкий участок находится между продажами, логистикой и документооборотом. Когда софт оценивают только по цене внедрения, такие потери остаются невидимыми. Когда оценивают по сквозному циклу, картина меняется моментально. Как считать эффективность по-взрослому

Я бы предложил для малого и среднего бизнеса очень прикладную формулу. Без сложных финансовых моделей, но с честной логикой. Эффект от софта = сокращение времени цикла, плюс сокращение ручного труда, плюс снижение ошибок и просрочек, плюс снижение

потерь сделок и клиентов, минус стоимость внедрения, поддержки и доработок. Теперь это можно приземлить.

1. Считаем время Если до внедрения заявка проходила путь от входящего обращения до счета за 6 часов, а после - за 2 часа, это не абстрактная красота. Это возможность обработать больше потока теми же людьми и быстрее закрывать деньги.

2. Считаем ручной труд Если три сотрудника ежедневно по часу переносят данные из одной системы в другую, это уже отдельная статья потерь. За месяц набегает десятки часов, которые выглядят как “мелочь”, пока их не переведут в фонд оплаты труда.

3. Считаем ошибки

Каждая ручная перебивка данных - это не только потерянные минуты. Это отмененная поставка, неверный счет, потерянный резерв, возврат, конфликт с клиентом и дополнительная нагрузка на руководителя.

4. Считаем упущенную выручку Очень часто дешевый софт не решает проблему пропущенных лидов, долгих согласований или поздних ответов клиенту. Формально он стоит меньше. Фактически он консервирует потери

Кейс 1. Дистрибьютор стройматериалов: когда хотели купить WMS, а нужно было лечить стыки Один из типовых кейсов - дистрибьюторский бизнес, около 120 сотрудников. Руководство готовилось вкладываться в складскую автоматизацию, потому что все жаловались на “медленный склад”. На поверхности картина выглядела логично: заказы отгружаются не так быстро, как хочется, менеджеры нервничают, клиент ждет. После разборки сквозной цепочки выяснилось неприятное: склад работал вполнeterпимо.

Проблема была не внутри склада, а на входе и выходе. Заказ из CRM передавали с задержкой. Логистика узнавала о готовности слишком поздно. Часть информации о резервах жила в таблицах и переписках. То есть компания собиралась лечить не то место.

Вместо дорогого проекта на первом этапе сделали три вещи: автоматическую передачу заказа из CRM без Excel, нормальный триггер для логистики при готовности, единый формат данных для последующих этапов.

Результат оказался значительно сильнее, чем ожидали от “большой” автоматизации: время ответа менеджера сократилось на 41%, потерянные сделки - на 23%, конверсия в счет

выросла в 1,6 раза. И это важный момент: эффект появился не потому, что компания купила еще одну систему, а потому, что убрала разрывы между уже существующими. Такой же кейс в сжатом виде есть и в наших публичных материалах: на сайте NeoGraph.tech мы показываем похожий дистрибьюторский сценарий с теми же симптомами - ручные Excel, неактуальные остатки и потеря сделок. (NeoGraph.tech)

Кейс 2. Сервисная сеть: дешевый helpdesk не спасает, если у вас нет контроля SLAB сервисном бизнесе проблема обычно выглядит иначе. Формально заявки поступают. Каналов связи много. Операторы отвечают. Но клиент все равно недоволен, потому что компания теряет управляемость на маршрутизации и сроках.

В одном из кейсов с сервисной сетью у бизнеса не было единой картины по слотам, заменам, эскалациям и просрочкам. Система как таковая присутствовала, норуководитель не видел, где заявка зависла, кто отвечает за переход между этапами и почему диспетчеры все время работают в режиме аврала. Здесь считать эффективность по цене лицензии было бы просто бессмысленно

Для такой цепочки важнее другие вопросы: на сколько сократилось количество просроченных SLA, сколько ручных уточнений ушло из работы, на сколько снизилась нагрузка на диспетчеров, улучшился ли опыт конечного клиента

После наведения порядка в маршрутизации и контрольных точках просроченные SLA снизились на 32%, нагрузка на диспетчеров - на 18%, а NPS вырос на 9 пунктов. Это хороший пример того, что софт полезен не тогда, когда у него длинный список модулей, а тогда, когда он начинает дисциплинировать процесс.

Кейс 3. Производство: BI без онтологии и триггеров часто превращается в красивый телевизор. С производством история еще интереснее.

**На заводах любят считать,
что если появились дашборды,
значит появилась цифровая
управляемость.**

К сожалению, это не так. В одном из производственных кейсов у клиента были отчеты, но не было понятной логики переходов и причинно-следственной карты процесса. План-факт собирался, согласования шли, данные копились, но руководители все равно поздно узнавали об отклонениях.

ВІ показывал симптомы, но не помогал вовремя действовать. После выстраивания цифровой онтологии процесса и триггерной отчетности время согласования сократилось на 28%, невыполнение плана - на 15%, а выработка смены выросла на 8%. Это тот случай, когда система начинает работать не как архив, а как инструмент действия. Для бизнеса это и есть настоящая эффективность. Пять ошибок, из-за которых софт не окупается

Ошибка 1. Считать только лицензию Самый дешевый продукт может оказаться самым дорогим, если под него приходится дорабатывать костыли, руками переносить данные и ежедневно компенсировать ограничения системы людьми

Ошибка 2. Автоматизировать один участок без карты всего процесса

Это классическая ловушка. Отдел становится быстрее. Компания - нет.

Ошибка 3. Не считать цену задержки У большинства компаний хорошо считается зарплата и плохо считается ожидание. Хотя ожидание на стыке часто и есть главный пожиратель маржи.

Ошибка 4. Путать внедрение с результатом Фраза “систему поставили” вообще ничего не говорит о пользе. Вопрос всегда один: что изменилось в деньгах, сроках, ошибках, конверсии, SLA и загрузке людей. Ошибка 5. Брать систему без владельца процесса Если никто не отвечает за сквозную цепочку, софт быстро становится еще одной витриной, которую все ругают, но никто не развивает. Что проверять до покупки софта Перед тем как подписывать договор, я бы советовал собственнику или руководителю пройти короткий список вопросов.

Где именно в процессе сейчас теряются деньги - внутри функции или на стыке? Какая метрика должна измениться после внедрения: время цикла обработки, конверсия, SLA, доля ошибок, загрузка команды? Сколько ручных действий система уберет уже в первый месяц? Какие данные по-прежнему будут жить в таблицах, чатах и почте? Кто владелец сквозного результата, а не только отдельного участка? Что будет считаться успехом через 90 дней после запуска? Если на эти вопросы нет ответа, значит бизнес пока выбирает не инструмент, а надежду. Что делать малому бизнесу, если бюджет ограничен Малому

бизнесу особенно опасно покупать большие системы по принципу “у всех стоит, и нам надо”.

У таких компаний меньше запас прочности и меньше права надолгую ошибку.

Я бы рекомендовал другой порядок: 1. Сначала нарисовать одну самую болезненную цепочку - например, от лида до оплаты

2. Зафиксировать 5-7 точек передачи данных между ролями.

3. Посчитать, где именно возникает ожидание, дублирование и ручной труд.

4. Выбрать одно узкое место, которое дает самый быстрый возврат

5. Только после этого покупать или дорабатывать софт.

Иногда после такого разбора оказывается, что бизнесу не нужна новая ERP. Нужны две интеграции, нормальный статусный контур и одно правило, которое убирает хаос на переходе между продажами и исполнением. Вывод: Эффективность софта нельзя честно посчитать по цене лицензии. Ее можно посчитать только по тому, как меняется живая экономика процесса. Хороший софт сокращает цикл, убирает ручные передачи, снижает число ошибок, дисциплинирует переходы между функциями и делает результат прозрачным для руководителя.

Плохой софт может стоить дешево, но при этом оставлять компанию в том же хаосе, только уже с красивым интерфейсом.

Поэтому главный вопрос перед покупкой всегда один и тот же: мы покупаем систему или убираем конкретную потерю в бизнесе?

Если ответа нет, считать ROI рано. Если ответ есть - цифры обычно становятся гораздо честнее.

*Александр Ожерельев, Генеральный директор **NeoGraph.tech**

Искусственный интеллект в системе документооборота и управления корпоративными процессами

Практический опыт внедрения нейросетей в корпоративные процессы

Введение

2026 год станет переломным для корпоративного управления. Если ещё год назад нейросети в офисе воспринимались как экспериментальная технология, то сейчас они встроены и продолжают встраиваться в повседневные процессы тысяч компаний. Но интеграция искусственного интеллекта (далее – ИИ) в документооборот — это не просто внедрение чат-ботов или замена программистов. Это принципиально иной подход к организации информационных потоков, управлению знаниями и контролю качества. Разговор об ИИ в документообороте часто упирается в одну из двух крайностей: либо руководители ждут магического решения, которое само разберётся со всеми бумагами, либо IT-отделы отмахиваются, что это не про нас — у нас есть Система Электронного Документооборота (далее – СЭД) и ее хватит. Обе позиции ошибочны. Нейросети в документообороте — это инструмент, который меняет экономику рабочего времени, повышает качество решений и создаёт аудиторский след, который раньше просто невозможно было создать. В этом материале — практический разбор того, как компании вводят ИИ-решения в работу с документами, какие ошибки чаще всего совершают, и как не потерять контроль над процессом в погоне за автоматизацией.

Почему AI критичен именно сейчас

Документооборот — это кровеносная система компании. Через документы движутся решения, риски, ответственность. В крупной организации человек, занимающийся



**Наталья
Абрамова**

эксперт по искусственному
интеллекту

обработкой входящих запросов, справок, претензий или согласований, тратит 60–70% времени на рутину: поиск нужного шаблона, заполнение полей, проверка соответствия требованиям, пересылка нужному отделу. Массовое внедрение ИИ-решений меняет экономику этого времени. Вместо того чтобы секретарь вручную заполнял форму согласования или юрист проверял договор на наличие критических пунктов, это делает система. Но главное — ИИ делает это не просто быстрее. ИИ делает это системнее. Возьмем конкретный пример. В крупной торговой сети приходит 150–200 входящих писем в день. Каждое нужно классифицировать: это претензия от клиента, запрос от партнёра, внутренний документ или спам. Потом каждое письмо нужно направить в нужный отдел. Человек на это тратит 3–4 часа в день и все равно ошибается в 5–7% случаев. Система классификации, обученная на примерах из реальной истории компании и встроенная в почтовый клиент или СЭД, делает то же самое за 2 минуты обработки всего потока — со скоростью около 100% точности. Второй момент: трассировка решений. Когда документ обрабатывает человек, невозможно проверить, почему именно это решение было принято. Когда это делает система, каждый шаг логирует — какие данные были проанализированы, какие правила применены, в какой момент. Это становится критичным для контроля качества, аудита и комплаенса. И как итог - масштабируемость знаний. Если в компании есть человек, который хорошо разбирается в тонкостях работы с определённым типом договоров, и он уходит, его знания уходят с ним. Если же эти знания встроены в алгоритм обработки документов, то система продолжает применять их последовательно, для каждого документа.

Практические направления внедрения

На основе опыта работы с разными компаниями я выделяю четыре основных направления, где внедрение ИИ-решений дает максимум эффекта.

1. Классификация и маршрутизация

Это самое простое, но невероятно эффективное применение. ИИ учится распознавать типы документов (счета, договоры, письма, жалобы, внутренние служебные записки) и либо классифицировать их в системе СЭД, либо сразу направлять в нужный отдел. Компании, которые внедрили такую систему в работу с почтой, отмечают, что время обработки входящего потока сокращается в 3–4 раза, а количество ошибок маршрутизации падает почти к нулю. При этом стоимость внедрения относительно низкая — не требуется переделывать всю СЭД, достаточно интеграции с существующим почтовым клиентом. GigaChat классифицирует 2,5 млн клиентских обращений в месяц в СберБанк Онлайн и госуслугах. В Московской области система обрабатывает 240 тыс. диалогов в год, направляя заявки в нужные ведомства за секунды. Точность маршрутизации — 97%. Время первого ответа сократилось с 8 до 2 минут. На входе — письмо или заполненная форма на сайте. Система должна понять: это реальная

заявка, заявка от злоумышленника или просто информационный запрос. На основании этого либо документ идет в работу кредитному отделу, либо уходит в папку спама/информационных запросов. До внедрения ИИ отдел кредитования вручную обрабатывал около 800 заявок в месяц. На классификацию и проверку на соответствие базовым требованиям уходило 40% времени каждого сотрудника. После внедрения системы те же 800 заявок поступают предварительно отсортированными, с рейтингом риска по каждой. Время на обработку упало на 35%. Критично: качество отбора улучшилось, потому что система не устаёт и не отвлекается.

2. Заполнение шаблонов и синтез документов

Здесь ИИ становится оператором - вместо того чтобы человек вручную заполнял договор или служебную записку по шаблону, система делает это, извлекая нужные данные из источников (CRM, аналитической системы, базы клиентов) и подставляя в нужные поля.

Типичный сценарий: в компании каждый день составляют от 20 до 100 писем-ответов на стандартные клиентские вопросы. Вместо того чтобы каждый раз писать письмо с нуля, система предлагает готовый текст, основанный на типе запроса, истории клиента и стандартных правилах компании. Человек только проверяет и отправляет. Одна из логистических компаний на этом получила значительный выигрыш. Они отправляют клиентам акты выполненных работ, накладные, счета. Раньше диспетчер для каждого заказа вручную собирал информацию из трех разных систем, заполнял форму, проверял цифры, отправлял. На один документ уходило 8–10 минут. С ИИ-синтезом документ генерируется за 30 секунд, после визуального контроля отправляется. Диспетчер теперь не заполняет документы — он контролирует качество. Это выглядит малым, но для команды из 10 человек это экономия 30–40 часов в неделю.

3. Анализ соответствия и выявление рисков

Здесь ИИ-инструмент становится экспертом. Система анализирует контракт на предмет соответствия внутренним стандартам компании, выявляет потенциальные риски, находит отклонения от шаблона и предупреждает об этом юриста.

Например, все договоры в компании должны содержать пункт о конфиденциальности, порядок расторжения и процедуру разрешения споров. Юрист загружает договор в систему. ИИ за 10 секунд проверяет наличие этих пунктов, анализирует их текст на предмет отклонений от стандартной практики компании и выдает отчет: «Пункт о конфиденциальности присутствует, формулировка совпадает со стандартом. Пункт о разрешении споров содержит отклонение: предусмотрен иностранный суд вместо арбитража РФ — требуется согласование с управлением рисков.» AI-агент на базе GigaChat сопоставляет коды бюджетной классификации. Система

анализирует финансовые документы на соответствие нормативам за секунды. Точность — 84%, что позволяет перевести рутинную сверку на машины. Для работы с договорами это критично. Юристы, которые внедрили такую систему, говорят, что это позволяет им за одно рабочее время проверить в два раза больше документов, не теряя в качестве. Более того, система выявляет ошибки, которые опытный юрист может пропустить просто из-за усталости.

4. Экспорт данных и синтез отчетности

Последнее направление, которое набирает популярность, — это обратная сторона документооборота. Не только прием и обработка, но и синтез из множества документов аналитики, отчетов и датасетов. Например, отдел контролирует соблюдение политики в отношении закупок. В системе СЭД хранятся тысячи заявок на закупку, каждая с разным статусом, суммой, поставщиком. Раньше аналитик выгружал данные в Excel, фильтровал, делал сводные таблицы. С ИИ это можно автоматизировать: система каждый день генерирует отчет о том, как много закупок проходит через нужную процедуру, какой процент заявок задерживаются, какие категории товаров чаще всего закупаются через исключения из регламента. На основе этого можно сразу видеть проблемы.

Рассмотрим примеры из практики

Кредитная компания

Задача была простой на вид: есть 500 отделений, в каждом обрабатывают документы физических лиц. Каждый день приходят заявления, справки, договоры. Часть документов неправильно заполнены, часть содержат опечатки, часть не соответствуют требованиям нормативов (152-ФЗ, правила компании). Ручная проверка каждого документа перед тем, как отправить его на следующий этап (кредитному отделу или архиву), занимала 15–20 минут. При объеме 300–400 документов в день на каждом отделении это означало, что один человек весь день занимается только проверкой.

Решение: встроили в СЭД модуль проверки документов. ИИ анализирует полноту заполнения, соответствие требованиям 152-ФЗ, логические ошибки и качество отсканированного изображения. Система выдаёт отчет: «Зеленый свет — документ соответствует требованиям; желтый свет — найдены потенциальные проблемы, требуется проверка; красный свет — документ не может быть обработан без исправлений». Результат: время обработки одного документа упало с 15–20 минут до 2–3 минут. Ошибок, которые попадают дальше в систему, практически нет. На каждом отделении появился дополнительный час рабочего времени в день на более ценные задачи. GigaChat в 2 раза ускорил анализ событий информационной

безопасности. Система классифицирует инциденты ИБ, готовит аннотации к отчетам и ищет аномалии в логах. Экономия времени аналитиков — 65%.

Производственная компания

В компании есть отдел, который ведет переписку с поставщиками и подрядчиками. Каждый день обновляются коммерческие предложения, меняются цены, появляются новые условия поставки. Это все нужно отслеживать, чтобы принимать решения о закупке. Раньше специалист вручную прошелся по всем письмам от поставщиков за неделю, выписал изменения в таблицу, сравнил с предыдущей неделей и подготовил отчет для руководства. Теперь система каждый день автоматически сканирует входящую почту, извлекает из писем информацию о ценах, условиях, сроках поставки, сравнивает с предыдущей информацией по каждому поставщику и выдает отчет, в котором видны все изменения. Это происходит каждый день и занимает буквально 5 минут. Польза здесь не столько в экономии времени, сколько в оперативности принятия решений. Раньше отчет готовился в конце недели, теперь информация свежая каждый день. Это позволяет компании быстрее реагировать на изменения на рынке.

Команда корпоративного обучения

При разработке программы обучения для сотрудников по использованию ИИ-инструментов в их работе встала задача: как персонализировать обучение так, чтобы каждому специалисту досталась информация, релевантная именно его функциям? В компании работает 300 человек, 7 отделов, каждый с разными задачами. Написать 7 разных программ обучения было бы слишком дорого. Решение - создали одну базовую программу с модулями. Система анализирует роль и функции каждого сотрудника (на основе его должности, истории писем, документов, которые он обрабатывает), и генерирует персонализированный путь обучения. Результат: уровень усвояемости материала вырос на 40%, потому что каждый видел примеры из своей работы.

Критические ошибки при внедрении

Опыт внедрения решений на базе ИИ в документооборот показал, что компании часто совершают одни и те же ошибки.

Ошибка 1: Внедрение без стратегии

Компания видит, что идет пик и тенденция использовать нейросети, и начинает что-то внедрять без четкого понимания: что мы автоматизируем? Какая польза ожидается? как

измерим результат? Как итог: система внедрена, потратили бюджет, но люди продолжают работать как раньше, потому что никто не переучил их, процессы не переделаны, а система просто параллельно крутится и накапливает ошибки. Правильный подход: сначала анализ — какие процессы съедают больше всего времени и ошибок? Потом пилот на одном отделении или на 10% операций. Потом масштабирование.

Ошибка 2: Полная автоматизация без контроля

Есть верхнеуровневый миф: «Внедрим ИИ и люди не будут нужны». На практике это опасно. Система может ошибаться. Система может быть скомпрометирована. Система может быть обучена на неполных данных. Правильный подход заключается в том, что это помощник, не замена. Система выдает рекомендацию, человек принимает решение. Система классифицирует документ, человек проверяет. Система заполняет форму, человек утверждает.

Ошибка 3: Игнорирование вопросов безопасности и комплаенса

Если в системе обрабатывают персональные данные (а в документообороте это практически всегда так), то система должна соответствовать 152-ФЗ. Это значит: данные не должны утекать, система должна вести логи всех операций, нужно согласие субъектов данных на обработку их данных через ИИ. Компании часто начинают с облачных сервисов, которые красиво работают, но не ясно, где хранятся данные и кто на них имеет доступ. Это опасно, но реализуемо. Инструменты, технологии не стоят на месте и решение находится под запрос.

Ошибка 4: Плохое качество обучающих данных

ИИ в целом мы уже все понимаем - это не волшебство. Система может быть только такой хорошей, как данные, на которых ее обучили. Если компания загрузила базу данных в систему из 10 000 примеров документов, но из них 3000 заполнены неправильно, то система научится ошибаться. ИИ итак не идеален и может галлюцинировать (ошибаться, вводить в заблуждение).

Правильный подход: перед обучением нужно почистить и разметить данные. Это долгий, скрупулезный, но критично важный этап внедрения.

Регулятивная сторона

При внедрении ИИ в документооборот компания попадает в поле регулирования Федерального закона № 152-ФЗ «О персональных данных». Практически любой корпоративный

документ содержит персональные данные: фамилии, контакты, реквизиты договоров. Это означает, что внедрение систем ИИ — не только технологический, но и юридический процесс.

Правовое основание. Любая обработка данных должна иметь правовое основание. Это может быть согласие субъекта, исполнение договора, трудовые отношения или требования закона. Компания должна чётко зафиксировать цели обработки, включая автоматизированный анализ.

Аудит и прозрачность. Системы должны логировать все операции: доступ к документам, действия пользователей, операции самой системы. Такие логи нужны для контроля качества и проверок регуляторов.

Защита данных. Законодательство требует применять меры безопасности: разграничение доступа, шифрование, защита каналов передачи, изоляция инфраструктуры. Компания несёт ответственность за безопасность данных — если утечка произойдёт через систему обработки документов, оператор обязан уведомить регулятора и устранить последствия.

Локализация и облако. При использовании облачных сервисов или зарубежных AI-платформ нужно учитывать требования локализации: данные граждан РФ должны обрабатываться на территории страны.

Отраслевые требования. Банк России издал рекомендации по использованию ИИ в финансовых организациях. Для банков это означает не только внедрение технологий, но и выстраивание процессов управления алгоритмическими рисками.

Таким образом, внедрение ИИ в документооборот — это комплексная задача на пересечении технологий, права и информационной безопасности. Только такой подход позволяет использовать потенциал ИИ без создания дополнительных рисков.

Как внедрять: пошаговая стратегия

Практика внедрения ИИ-решений в документооборот показывает, что наилучшие результаты достигаются при поэтапном подходе. Такой подход позволяет снизить технологические и организационные риски и постепенно интегрировать новые инструменты в существующие процессы.

Шаг 1. Аудит процессов. На первом этапе необходимо проанализировать, какие типы документов обрабатываются в компании, какие операции выполняются с ними и сколько времени занимают основные этапы обработки. Важно также определить, где возникают ошибки и задержки. Такой аудит обычно можно провести в течение одной-двух недель на уровне отдельного подразделения.

Шаг 2. Выбор пилотного сценария. По результатам аудита выбирается одно направление для пилотного внедрения. Чаще всего компании начинают с задач классификации и маршрутизации документов: такие решения дают быстрый эффект и требуют меньшей подготовки инфраструктуры.

Шаг 3. Подготовка данных. Следующий этап — формирование обучающего набора данных. Для этого собираются типовые документы, которые система будет обрабатывать, и выполняется их разметка: указывается тип документа, ключевые поля и другие параметры, необходимые для обучения модели. Качество подготовки данных напрямую влияет на точность работы системы.

Шаг 4. Пилотное внедрение. После подготовки данных запускается пилотный проект — например, в одном подразделении или на ограниченном объеме операций. На этом этапе важно отслеживать ключевые метрики: скорость обработки документов, точность распознавания, количество ошибок и удобство работы для пользователей.

Шаг 5. Доработка решения. Результаты пилота позволяют определить, какие элементы системы требуют доработки. Это может быть расширение перечня типов документов, повышение точности моделей или интеграция с корпоративными системами.

Шаг 6. Масштабирование. После успешного пилота решение разворачивается на уровне всей организации или сети подразделений. Одновременно проводится обучение сотрудников и выстраивается процесс технической поддержки.

Шаг 7. Оптимизация и развитие. Даже после масштабирования система требует регулярной настройки. По мере накопления новых данных можно улучшать алгоритмы, повышать точность обработки документов и расширять функциональность.

Как показывает практика, полный цикл внедрения — от аудита процессов до масштабного использования — обычно занимает от шести до двенадцати месяцев. Это не самый быстрый путь, но именно такой подход позволяет внедрять ИИ-решения устойчиво и без существенных операционных рисков.

Практические советы

1. Начните с малого. Не пытайтесь сразу автоматизировать весь документооборот. Выберите один процесс, который занимает много времени, и решите его. После успеха будет проще убедить людей внедрять дальше.

2. Обучайте людей. Большая часть сопротивления новым системам связана не с технологией, а с незнанием. Люди не знают, как работает система, не доверяют ей, боятся, что станут безработными. Потратьте время на обучение.

3. Ведите метрики. Не включайте систему и не забывайте о ней. Отслеживайте: ускорила ли работа? снизились ли ошибки? что говорят пользователи? На основе метрик принимайте решения о развитии.

4. Думайте о безопасности с самого начала. Не добавляйте комплаенс потом. Если система с самого начала не защищает данные, то потом переделывать будет дорого и больно.

5. Ищите партнеров и консультантов. Не делайте это в одиночку. Обсуждайте с коллегами из других компаний, читайте, привлекайте консультантов. Это сэкономит время и ошибки.

Заключение

ИИ в документообороте — это не тренд, это реальность. Компании, которые сейчас начинают внедрение, получают преимущество в эффективности и качестве работы. Компании, которые будут ждать, когда технология созреет окончательно, рискуют отстать. Но это не значит, что нужно внедрять всё подряд. Нужен стратегический подход: понять, где острая необходимость, выбрать нужное решение, правильно его внедрить, обучить людей, отслеживать результаты. ИИ — это инструмент. Как и любой инструмент, он может быть использован хорошо или плохо. Ключ к успеху — это понимание того, что делаешь и зачем. Компании, которые сейчас управляют этим процессом осознанно, будут конкурировать в 2027–2030 годах не только на цену, но и на скорость, качество и надежность. Это мощное преимущество.

***Наталья Абрамова**, эксперт по искусственному интеллекту и информационной безопасности, амбассадор безопасного ИИ, руководитель стратегических проектов в сфере ИИ и ИБ, CEO медиа-платформы «НЕЙРОЭРА»

КОНФЕРЕНЦИЯ УПРАВЛЕНИЕ УПРАВЛЕНЦАМИ



Екатерина Мартьянова, известный эксперт
**Личный бренд управленца: как имя влияет
на авторитет и результаты команды**

Валерия Гришко, Supulat

Как можно наказывать топов управленцев?



Елена Буланова, Основатель коммуникационной
группы Mimicry group

Секреты управления управленцами

Федор Васильев,
АО «ГЛАВСНАБ»

Как можно наказывать топов управленцев?



Екатерина Пинто, эксперт в области трудовых
отношений, независимый эксперт

Виктория Раневская,
Есть контакт! CEO



Татьяна Моисеева, Директор ООО МАРКЕТ ГРУПП

23.04 С 16.00 ДО 19.00

УЧАСТИЕ 3000 РУБ

для подписчиков  **БЕСПЛАТНО**

ЗАПИСЬ – 7447273@VK.RU, 89258817901,

ТГ @NADYAGONCHAROVA_ONCONNECT

БИЗНЕС
ИДЕИ

БИЗНЕС
РЕШЕНИЯ

БИЗНЕС
ТЕХНОЛОГИИ

БИЗНЕС
ПРОЦЕССЫ

WWW.TOP-PERSONAL.RU

№ 11
(915)

2026

УПРАВЛЕНИЕ ПЕРСОНАЛОМ

Авторский журнал по управлению персоналом - 7062, 7063, 7205.



Асланов
Тимур



Былинкин
Сергей



Баранова
Татьяна



Батырев
Максим



Валинуров
Ильгиз



Вашенко
Андрей



Гаврилова
Надежда



Гандапас
Радислав



Лузенюк
Филипп



Ерин
Дмитрий



Ерохин
Александр



Жигилий
Евгений



Колотилев
Евгений



Кривулин
Игорь



Кроль
Леонид



Кукушкин
Марк



Курч
Андрей



Манн
Игорь



Мушин-
Македонский
Артём



Набок
Оксана



Непрыхин
Никита



Норка
Дмитрий



Овчаренко
Максим



Петрова
Виктория



Семенов
Сергей



Сёмин
Дмитрий



Соломатин
Александр



Ткаченко
Дмитрий



Тютин
Альберт



Габдулла
Хамитов



Юстус
Генрих



Яхонтова
Елена

Главная тема: Лучшие бизнес-тренеры и бизнес-консультанты



Ваш персональный искусственный интеллект в сфере HR

Не где-то там, наверху, а именно Ваш, персональный, живущий на вашем рабочем месте.

И ожидающий Вашего приказа, чтобы сделать работу точнее, быстрее и приятнее.

С удивительными результатами - на то он и искусственный интеллект новейшего поколения.

Подробнее о подходе см. журнал УП 2'2026, материалы конференции поиска талантов и пр.

Заведите себе персональный ИИ - его не нужно выгуливать, но желательно кормить свежей информацией.

Можно предварительно с ним познакомиться - посмотреть, потискать, поработать вживую - выездные учебно-практические семинары по всей России и СНГ.

Такого раньше вообще не было, а теперь есть. И ждет Вас!

НПО ЭТАЛОН - 24 года успешной работы в России и за рубежом

+7 915 010-46-90

www.npo-etalon.ru