СТРАТЕГИЧЕСКИЙ ОТЧЁТ · ИЮЛЬ 2026 ГОДА

Мёртвый интернет

От пугающей метафоры к управляемому бизнес-риску

Сводный анализ исследований Perplexity и Qwen, независимая проверка ключевых утверждений и план действий до 2031 года

ДОВЕРИЕ · ЧИСТЫЕ ДАННЫЕ · ПРЯМАЯ АУДИТОРИЯ

Для владельцев бизнеса и высшего руководства

Подготовлено для toritsyn.com

Резюме для принятия решений

> **Главный вывод.** Интернет не стал безлюдным, но машинные запросы уже превысили человеческие в нескольких крупных измерительных контурах. Для бизнеса это означает не конец цифровых каналов, а конец доверия к необработанным показам, кликам, заявкам и открытым данным.

53%	74,2%	68,01%
доля автоматических запросов	**страниц с машинной помощью**	**поисков без перехода**
Талес, трафик за 2025 год	Арефс, 900 000 новых страниц	СпаркТоро, первые 4 месяца 2026 года

Эти три числа нельзя складывать и нельзя трактовать как долю «неживого интернета». Они описывают разные явления: запросы к серверам, признаки машинной помощи в тексте и отсутствие перехода из поиска. Вместе они показывают один структурный сдвиг: привычная цепочка «человек увидел — человек нажал — компания получила данные» больше не является надёжной моделью по умолчанию.

Оба исследования верно фиксируют направление изменений: автоматический трафик стал большинством, производство содержимого резко подешевело, открытый поиск возвращает меньше переходов, а доверие и собственная аудитория превращаются в самостоятельные активы. При этом формула «теория доказана» слишком категорична. Боты включают полезных поисковых роботов, помощников покупателей, средства наблюдения за доступностью и интеграции между системами. Риск определяется намерением, экономическим эффектом и возможностью подтвердить источник, а не самим фактом автоматизации.

Шесть решений для владельца и совета директоров

1. **Пересчитать экономику привлечения.** Утвердить два набора показателей: все события и подтверждённые человеческие события. Бюджетировать по второму набору.
2. **Назначить владельца качества цифрового трафика.** Ответственность должна быть общей для маркетинга, информационной безопасности, аналитики и финансов, а не растворяться между подрядчиками.
3. **Защитить программные интерфейсы и формы.** Перейти от одной проверки на человека к многослойной оценке поведения, репутации источника, скорости запросов и риска операции.
4. **Перестроить распространение содержимого.** Оптимизировать материалы не только ради перехода из поиска, но и ради корректного цитирования системами ответов; параллельно наращивать рассылки, закрытые сообщества и прямые контакты.
5. **Ввести происхождение данных.** Каждый источник для аналитики и корпоративных моделей должен иметь владельца, дату, уровень доверия, историю преобразований и правила допуска.

6. **Подготовить прозрачность машинного содержимого.** Для компаний, работающих в Европейском союзе, требования статьи 50 становятся применимыми 2 августа 2026 года; для остальных маркировка и редакционная ответственность уже полезны как защита бренда.

План первых 90 дней

Срок	Что сделать	Владелец	Результат
0–30 дней	Разметить автоматический трафик, перепроверить рекламные события, составить карту машинного содержимого и внешних данных.	Маркетинг, безопасность, данные	Исходная точка и перечень утечек бюджета
31–60 дней	Запустить независимую проверку трафика, защитить критичные формы и интерфейсы, отделить проверенные данные от открытых.	Технологии и финансы	Сопоставимые показатели до и после защиты
61–90 дней	Перераспределить расходы, запустить канал прямой аудитории, утвердить правила происхождения содержимого и данных.	Генеральный директор	Решение о масштабировании и целевые показатели

1. Предмет анализа и границы вывода

1.1. Что именно изучено

В основу отчёта положены два приложенных материала: аналитический отчёт Perplexity в формате документа и исследование Qwen в формате публикации. Оба материала охватывают экономику автоматических ферм, влияние на рекламу и поиск, кризис доверия, миграцию в закрытые сообщества, угрозы корпоративным моделям и сценарии до 2031 года.

Дополнительно проверены наиболее важные утверждения по первичным или максимально близким к первичным источникам: отчёт Талес о трафике за 2025 год, данные сети Клаудфлэр, исследование Арефс по 900 000 страницам, исследования СпаркТоро и Семраш по поискам без перехода, работа в журнале Nature о деградации моделей, эксперимент в Трудах Национальной академии наук, исследование Энтропик об отравлении данных, официальный текст статьи 50 европейского закона и техническое описание стандарта происхождения содержимого.

1.2. Как оценивалась надёжность

Уровень	Что означает	Как используется в отчёте
А — подтверждено	Первичный источник, раскрытая методика, понятный знаменатель.	Можно применять как основание для решения с указанными ограничениями.
Б — сильный сигнал	Крупный поставщик данных или исследование, но выборка ограничена собственной сетью либо методом распознавания.	Используется для направления и внутренней проверки, а не как универсальная истина.
В — оценка рынка	Расчёт поставщика услуги, вторичная публикация или широкий диапазон без единой методики.	Показывается диапазоном; требует проверки на данных компании.
Г — сценарий	Прогноз, экспертная гипотеза или экстраполяция до 2031 года.	Используется для подготовки, но не для обещания финансового результата.

> **Правило чтения.** Чем ярче число, тем важнее его знаменатель. Доля запросов не равна доле людей, доля страниц не равна доле внимания, а потери рынка не равны потерям конкретной компании.

1.3. Сильные и слабые стороны двух исследований

Критерий	Исследование Perplexity	Исследование Qwen
Сильная сторона	Чёткая управленческая структура, компактные таблицы, практический план защиты и маркетинга.	Более широкий социальный и инфраструктурный контекст, подробный сценарий двухуровневого интернета.

Критерий	Исследование Perplexity	Исследование Qwen
Главное ограничение	Некоторые рыночные оценки и показатели доверия даны как факты без достаточного акцента на методике.	Список источников чрезмерно широк и включает сообщения в сетях, ролики и коммерческие обзоры; часть причинных связей заявлена сильнее доказательств.
Полезный вклад	Связывает качество трафика с экономикой рекламы, поиска и корпоративных данных.	Показывает, как доверие, цифровая идентичность и закрытые сообщества могут стать инфраструктурой рынка.
Как использовано	Каркас операционных мер и перечень показателей.	Сценарии, социальные последствия и долгосрочные варианты развития платформ.

2. Что означает «мёртвый интернет» для бизнеса

Полезное рабочее определение: «мёртвый интернет» — это цифровая среда, в которой существенную часть запросов, публикаций, взаимодействий и сигналов создают программы, а компания не может надёжно отделить полезную автоматизацию, вредоносную автоматизацию и действия людей. Это определение измеримо и превращает метафору в набор управляемых рисков.

2.1. Чего вывод не означает

- Люди не исчезли из сети. Они всё чаще получают ответ без перехода на сайт, общаются в личных сообщениях и закрытых группах, используют помощников как посредников.
- Любой бот не является вредителем. Поисковые роботы, средства доступности, наблюдение за работой систем и помощники клиентов создают ценность.
- Машинное содержимое не обязательно низкокачественное. Исследование Арефс обнаружило признаки машинной помощи на 74,2% новых страниц, но только 2,5% были классифицированы как полностью машинные; сам детектор не безошибочен.
- Открытая сеть не исчезает мгновенно. Её экономическая роль меняется: она становится источником данных для ответных систем и автономных помощников, а переход к владельцу источника происходит реже.

2.2. Что действительно изменилось

Раньше сайт одновременно был витриной, каналом привлечения и точкой измерения. Теперь видимость может возникать внутри чужой ответной системы, действие может выполнять программный помощник, а посещение сайта может не состояться. Следовательно, компании необходимо управлять тремя слоями отдельно: доступом машин к содержимому, доказательством ценности бренда в ответах и подтверждением человеческой ценности событий.

3. Карта фактов: что подтверждено, а что требует осторожности

3.1. Автоматический трафик стал большинством

Отчёт Талес за 2026 год, основанный на трафике за 2025 год, сообщает: автоматические программы создали более 53% веб-трафика, люди — 47%, а вредоносные программы — 40%. Годом ранее соответствующая серия отчётов оценивала автоматическую долю в 51%. Клаудфлэр в июле 2026 года также сообщила о переходе машинного трафика через половину в собственной сети и отметила, что 52% запросов распознанных роботов в июне 2026 года были связаны с обучением систем.

> **Ограничение.** Талес и Клаудфлэр видят огромные, но разные части сети и применяют собственные классификаторы. Это оценки доли запросов, а не количества посетителей. Один автоматический агент может создать тысячи запросов, тогда как человек — несколько десятков.

Показатель	Значение	Надёжность	Правильная трактовка
Автоматические запросы	53%	Б	Большинство трафика в измерительном контуре Талес за 2025 год.
Вредоносные запросы	40%	Б	Высокий риск для защищаемых приложений; не универсальная доля всех посещений.
Нечеловеческий трафик	более 50%	Б	Порог пройден в данных Клаудфлэр; точная доля зависит от среза.
Запросы роботов для обучения	52%	Б	Доля среди распознанных запросов роботов Клаудфлэр в июне 2026 года.

3.2. Производство содержимого стало почти бесплатным

Арефс проверила 900 000 англоязычных страниц, впервые замеченных её роботом в апреле 2025 года, по одной странице на домен. Детектор нашёл признаки машинного текста на 74,2% страниц: 71,7% были смешанными и 2,5% — полностью машинными. Это сильный сигнал о распространении инструментов, но не доказательство того, что три четверти всей сети созданы без участия человека.

Экономический механизм очевиден: предельная стоимость ещё одной статьи, изображения, отзыва или рекламного варианта приблизилась к нулю. Поэтому предложение информации растёт быстрее внимания. Дефицитом становятся не слова, а проверяемый опыт, первичные данные, репутация автора, доступ к аудитории и право на использование содержимого.

3.3. Поиск удерживает ответ у себя

СпаркТоро оценил, что 68,01% поисков в крупнейшей поисковой системе в первые четыре месяца 2026 года закончились без перехода на внешний сайт. Семраш на выборке почти из 69 млн. поисковых сеансов с мая по июль 2025 года оценил долю поисков без перехода в режиме ответа с искусственным интеллектом примерно в 93%. Эти результаты нельзя переносить на каждую страну, отрасль и тип запроса, но они подтверждают: место в выдаче всё чаще даёт видимость без посещения.

> **Управленческий смысл.** Поисковая оптимизация не исчезает. Её цель расширяется: быть найденным, быть правильно понятым и быть процитированным, а затем переводить узнаваемость в прямой контакт там, где это возможно.

3.4. Потери от рекламного мошенничества велики, но диапазон ненадёжен

В приложенных исследованиях встречаются оценки от 37,7 млрд. до 250 млрд. долларов в год, а также прогноз 172 млрд. долларов к 2028 году. Это оценки поставщиков средств защиты и отраслевых компаний с разными определениями недействительного трафика, каналами, странами и моделями пересчёта. Использовать верхнюю границу как установленный факт нельзя.

Для конкретного бизнеса важнее четыре собственных числа: доля подтверждённо недействительных событий, стоимость подтверждённого человека, доля заявок с реальным намерением и прирост продаж по сравнению с контрольной группой. Именно они должны определять перераспределение расходов.

3.5. Доверие и закрытые сообщества

Оба исследования указывают на миграцию общения в личные сообщения, рассылки, закрытые группы и тематические сообщества. Направление правдоподобно и согласуется с публичными наблюдениями платформ, но часто цитируемые «84% закрытого обмена» имеют неясную актуальность и методику. Поэтому в настоящем отчёте показатель не используется как текущая глобальная доля.

Надёжный вывод уже достаточен для действия: чем хуже проверяется публичный охват, тем ценнее каналы, где компания знает источник согласия, историю участия и качество связи. Однако закрытая группа сама по себе не гарантирует человечность: в неё также проникают автоматические аккаунты, мошенники и искусственная вовлечённость. Нужны правила входа, модерация и измерение удержания.

4. Экономические последствия по цепочке создания ценности

4.1. Привлечение и реклама

Главная проблема — не только прямое списание денег за фиктивный клик. Машинные события обучают автоматическое распределение бюджета. Если система считает бота хорошим потенциальным клиентом, она ищет похожие профили, повышает ставки и масштабирует ошибку. Возникает петля: плохой сигнал создаёт плохую оптимизацию, а плохая оптимизация производит ещё больше плохих сигналов.

- **Финансовый риск.** Расходы уходят на события без вероятности выручки; стоимость реального клиента скрывается внутри средней цены.
- **Аналитический риск.** Сравнение каналов становится ложным, если уровень автоматического трафика различается.
- **Репутационный риск.** Автоматическая закупка может размещать бренд рядом с дезинформацией и низкокачественными страницами.
- **Операционный риск.** Ложные заявки загружают продажи и поддержку, ухудшают скорость ответа реальным клиентам.

4.2. Поиск и издательская экономика

Ответные системы разрывают прежний обмен: владелец сайта отдаёт доступ к знаниям, но не обязательно получает посещение, рекламу или партнёрскую продажу. Уникальные данные и авторитет могут быть процитированы, но ценность останется у посредника, если бренд не умеет измерять присутствие в ответах и переводить его в подписку, запрос цены или прямое обращение.

Для издателей и экспертных компаний возникает новая лицензируемая ценность: структурированные данные, свежесть, проверяемое авторство и право использования. Клаудфлэр отмечает более 50 соглашений между издателями и компаниями искусственного интеллекта с 2023 года. Пока такие сделки не заменяют потери от переходов, но показывают возникновение рынка доступа к качественным данным.

4.3. Корпоративные данные и модели

Открытая сеть становится менее однородным источником. Риск состоит из двух разных механизмов. Первый — случайное загрязнение: повторяющиеся машинные тексты сужают разнообразие и вытесняют редкие факты. Второй — намеренное отравление: злоумышленник внедряет документы, рассчитанные на изменение поведения модели или системы поиска по внутренним знаниям.

Исследование Энтропик совместно с британским институтом безопасности искусственного интеллекта и Институтом Алана Тьюринга показало, что в их эксперименте 250 вредоносных документов, около 0,00016% обучающих единиц крупнейшей выборки, могли внедрить узкую скрытую реакцию. Авторы проверяли модели до 13 млрд. параметров и подчёркивали ограниченность конкретного сценария. Это не означает, что любые 250 страниц «ломают» любую систему, но означает, что простое увеличение объёма чистых данных не является достаточной защитой.

Работа в Nature подтверждает риск деградации, когда новые поколения моделей рекурсивно обучаются на результатах предыдущих. Одновременно другие исследования показывают, что сохранение и накопление реальных данных может существенно снизить риск. Практический вывод для бизнеса — не запрещать синтетические данные, а маркировать их, сохранять эталонные человеческие наборы и проверять качество на реальных задачах.

4.4. Бренд и доверие

Когда аудитория не уверена, человек ли автор, каждая коммуникация платит «налог на недоверие»: читатель тратит время на проверку, игнорирует слишком гладкий текст или просит подтверждение у знакомых. Побеждает не тот, кто производит больше сообщений, а тот, кто быстрее доказывает источник, ответственность и опыт.

Стандарт происхождения цифрового содержимого позволяет криптографически связать файл с историей создания и изменений. Он подтверждает целостность заявленной истории, но не истинность самого утверждения. Подписанное ложное изображение остаётся ложным. Поэтому техническое происхождение должно дополняться редакционной ответственностью, ссылками на данные и понятным способом исправления ошибок.

4.5. Право и соответствие требованиям

Статья 50 европейского закона требует, среди прочего, машиночитаемой маркировки синтетических материалов поставщиками систем, информирования человека о взаимодействии с машиной и раскрытия искусственного происхождения подделок и некоторых текстов по общественно значимым вопросам. Правила становятся применимыми 2 августа 2026 года и содержат исключения, в том числе для обычного редактирования и материалов под редакционной ответственностью. Окончательную применимость к компании должен определять юрист по конкретным ролям, рынкам и видам содержимого.

5. Риски по функциям и отраслям

Функция	Главный риск	Первое действие	Показатель контроля
Маркетинг	Фиктивные показы, клики и заявки обучают неверную закупку.	Параллельно считать все и подтверждённые события.	Стоимость подтверждённого клиента

Функция	Главный риск	Первое действие	Показатель контроля
Продажи	Ложные обращения занимают время и искажают прогноз.	Оценивать признаки намерения и подтверждать контакт.	Доля принятых отделом продаж заявок
Безопасность	Автоматические атаки идут через вход, формы и программные интерфейсы.	Риск-оценка поведения и ограничение частоты по операции.	Доля заблокированных вредоносных действий
Данные	Открытые источники загрязняют показатели и знания.	Реестр происхождения и уровни доверия.	Доля данных с владельцем и историей
Финансы	Счета подрядчиков не связаны с подтверждённым результатом.	Сверять оплату с проверенными событиями и продажами.	Расход на подтверждённую выручку
Право	Непрозрачное машинное содержимое и взаимодействие.	Карта ролей и обязанностей по рынкам.	Доля материалов с корректной маркировкой

5.1. Приоритет по типу бизнеса

Тип бизнеса	Наиболее уязвимое место	Стратегический ответ
Интернет-торговля и билеты	Сбор цен, захват остатков, фиктивные корзины, злоупотребление входом.	Защищать операции, а не только страницы; различать полезных помощников покупателей и злоумышленников.
Финансовые услуги	Подбор паролей, захват учётных записей, мошеннические заявки.	Усиленная проверка риска, защищённые ключи входа, подтверждение критических действий.
Средства массовой информации	Падение переходов и бесплатное извлечение содержимого.	Лицензирование, прямые подписки, данные о востребованности материалов у машинных систем.
Деловые услуги и программные продукты	Машинные заявки и потеря видимости в поиске.	Проверка намерения, оригинальные исследования, присутствие в ответных системах, сообщества специалистов.
Площадки и объявления	Автоматические аккаунты, отзывы, цены и взаимодействия.	Репутация участника, подтверждение личности по риску, стоимость доверенной сделки.
Потребительские бренды	Поддельные отзывы, искусственная аудитория авторов, соседство с мусорным содержимым.	Проверка аудитории партнёров, происхождение медиа, собственная база согласий.

6. Сценарии до 2031 года

Исследования сходятся в идее двух слоёв: открытой машинной среды и доверенных человеческих пространств. Это полезная модель, но не единственный возможный исход. Ниже четыре сценария. Они не являются взаимоисключающими: разные отрасли и страны могут двигаться по разным траекториям.

Сценарий	Что происходит	Ранние признаки	Ответ бизнеса
Управляемое разделение	Машинные запросы доминируют, но идентифицируются; доступ и оплата содержимого становятся договорными.	Подписанные роботы, раздельные права на поиск и обучение, лицензии данных.	Настроить правила доступа и цену качественных данных.
Закрытые сады	Крупные платформы удерживают ответы, торговлю и общение внутри экосистем.	Снижение внешних переходов, рост встроенных покупок и закрытых каналов.	Не зависеть от одного посредника; наращивать прямую аудиторию.
Премия за человечность	Проверенный автор, живое событие и личная рекомендация становятся дорогим дефицитом.	Рост платных сообществ, мероприятий, экспертных форматов и подтверждённого происхождения.	Инвестировать в доказуемый опыт и отношения, а не в объём публикаций.
Кризис доверия	Автоматизация и мошенничество опережают защиту; показатели и открытые данные теряют полезность.	Рост возвратов, ложных заявок, споров о происхождении и регуляторных ограничений.	Сократить зависимость от открытых сигналов, усилить подтверждение и резервные каналы.

6.1. Базовый сценарий

Наиболее вероятна комбинация первых трёх сценариев: автоматические помощники становятся обычным способом доступа, платформы удерживают всё больше пути клиента, а доверенные человеческие пространства получают ценовую премию. Публичная сеть остаётся витриной и сырьевой базой, но сделки, лояльность и глубокое знание клиента переходят в пространства с подтверждённой историей отношений.

6.2. Поворотные сигналы для ежегодного пересмотра стратегии

- Доля подтверждённых автоматических запросов и их экономический эффект по критичным операциям.
- Доля выручки, начавшейся без прямого посещения сайта или через машинного помощника.
- Доля материалов бренда, корректно цитируемых ответными системами.
- Стоимость подтверждённого человеческого контакта по каждому каналу.

- Число рынков, где маркировка и происхождение машинного содержимого стали обязательными.
- Доля внешних данных, прошедших проверку происхождения до использования в корпоративных моделях.

7. Целевая модель: инфраструктура цифрового доверия

Защита не должна сводиться к блокировке всего машинного. Компаниям нужны полезные помощники, поиск, интеграции и средства доступности. Целевая модель принимает решение по четырём вопросам: кто обращается, что пытается сделать, имеет ли право, каков экономический и безопасностный риск.

Слой	Возможности	Минимальный результат
Наблюдение	Единые журналы запросов, событий рекламы, заявок, продаж и атак.	Можно связать источник с реальным результатом.
Классификация	Человек, полезная программа, неизвестная программа, вредоносная программа.	Отчётность не смешивает разные типы трафика.
Решение	Разрешить, замедлить, запросить дополнительное подтверждение, ограничить или заблокировать.	Трение соответствует ценности и риску операции.
Происхождение	Владелец данных, дата, лицензия, история преобразований, уровень доверия.	В модели и отчёты попадают только допустимые источники.
Доказательство	Подписанное содержимое, редакционная ответственность, ссылки на первичные данные.	Аудитория может проверить источник и исправления.
Прямая связь	Рассылка, личный кабинет, сообщество, мероприятия, договорные контакты.	Бренд не теряет аудиторию при изменении алгоритма посредника.

7.1. Принципы защиты от автоматического трафика

- **Не доверять адресу сети как личности.** Резидентские посредники и распределённые устройства делают адрес слабым сигналом.
- **Оценивать поведение и намерение.** Скорость, последовательность, повторяемость, история устройства и риск операции полезнее одной загадки.
- **Создавать ступени трения.** Простой просмотр должен оставаться лёгким, а дорогая или необратимая операция — требовать более сильного подтверждения.
- **Защищать программные интерфейсы отдельно.** Ограничение частоты, токены доступа, подпись запросов, привязка к операции и наблюдение за бизнес-логикой обязательны.

- **Сохранять путь для полезных машин.** Известным помощникам нужен прозрачный способ представиться, объявить цель и соблюдать ограничения.

7.2. Новая модель маркетинга

Стратегия смещается от максимального охвата к подтверждённому вниманию. Это не отказ от рекламы и поиска, а изменение единицы покупки: компания платит не за абстрактный клик, а за проверяемый прирост человеческого действия.

Старая привычка	Новая практика	Почему
Оптимизировать по всем конверсиям	Оптимизировать по подтверждённым продажам или качественным заявкам	Автоматические события иначе усиливают сами себя.
Публиковать больше статей	Публиковать первичные данные, опыт, методику и обновления	Объём стал дешёвым; доказуемая уникальность остаётся редкой.
Считать только позиции в поиске	Считать цитирование, точность ответа, брендовый спрос и прямые обращения	Видимость всё чаще не приводит к переходу.
Арендовать аудиторию у платформ	Строить базу согласий и сообщества	Прямой канал устойчивее к смене алгоритма.
Выбирать автора по числу подписчиков	Проверять состав аудитории и прирост продаж	Численность легко автоматизировать.

8. Подробная программа первых 90 дней

Этап 1. Диагностика — дни 1–30

7. Назначить руководителя программы и рабочую группу из маркетинга, безопасности, данных, финансов, продаж и права.
8. Выбрать пять наиболее дорогих цифровых путей: рекламный переход, регистрация, заявка, вход, покупка или иная критичная операция.
9. Для каждого пути связать журналы запросов, рекламные метки, данные формы, систему продаж и факт выручки.
10. Разделить события на подтверждённо человеческие, полезные автоматические, вредоносные и неизвестные; зафиксировать долю неизвестных.
11. Провести выборочную ручную проверку дорогих источников трафика и партнёров.
12. Составить карту всех мест, где создаётся машинное содержимое или используются внешние данные.

Этап 2. Защита и эксперимент — дни 31–60

13. Включить поведенческую оценку и ограничение частоты на критичных формах и программных интерфейсах.
14. Запустить независимое измерение недействительного трафика минимум на двух сопоставимых каналах.
15. Создать контрольную группу или период, чтобы измерить прирост, а не просто число событий после фильтрации.
16. Ввести белый список источников корпоративных знаний и карантин для новых внешних документов.
17. Опубликовать шаблон раскрытия машинной помощи: что создано машиной, кто проверил, кто отвечает за результат.
18. Подготовить один материал с первичными данными и разметкой, пригодной для точного машинного цитирования.

Этап 3. Решение и масштабирование — дни 61–90

19. Перераспределить расходы по стоимости подтверждённого результата; не использовать общий уровень мошенничества как поправку без данных компании.

20. Зафиксировать договорные требования к рекламным площадкам и подрядчикам: определение недействительного события, доступ к журналам, порядок компенсации и срок расследования.
21. Запустить канал прямой аудитории с явным согласием: рассылку, закрытое сообщество или программу клиентов.
22. Утвердить политику происхождения данных и содержимого, включая срок хранения, лицензию, владельца и правила удаления.
23. Представить совету директоров базовую линию, эффект пилота, остаточный риск и бюджет следующего этапа.

9. Панель руководителя

Панель должна быть короткой и связывать качество цифровых сигналов с деньгами. Рекомендуется показывать медиану и диапазон, сравнение с контрольной группой и отдельную долю неизвестного трафика.

Показатель	Формула или смысл	Частота	Тревожный сигнал
Доля подтверждённых людей	Человеческие сеансы / все сеансы	Еженедельно	Падает при неизменном бюджете
Доля неизвестных	Неклассифицированные события / все события	Еженедельно	Выше установленного порога риска
Стоимость подтверждённого клиента	Расход канала / новые подтверждённые клиенты	Ежемесячно	Растёт быстрее валовой прибыли
Качество заявок	Принятые продажи / все заявки	Еженедельно	Снижается после масштабирования
Прирост выручки	Разница с контрольной группой	По кампании	Отсутствует при высоком числе конверсий
Прямая аудитория	Активные согласившиеся контакты и удержание	Ежемесячно	Рост базы без роста активности
Точность машинных ответов	Доля проверенных ответов с корректным описанием бренда	Ежемесячно	Ключевые факты искажены
Происхождение данных	Допущенные наборы с владельцем и историей / все наборы	Ежеквартально	Открытые данные входят без проверки

9.1. Правила остановки

- Приостановить масштабирование канала, если рост заявок не подтверждается ростом принятых продаж или контрольным экспериментом.

- Усилить проверку операции, если ущерб от автоматизации превышает стоимость дополнительного трения для реальных клиентов.
- Вывести источник данных из эксплуатации, если невозможно установить владельца, лицензию, дату и путь преобразований.
- Остановить автоматическую публикацию, если редакционная ответственность не назначена или исправления нельзя проследить.
- Не блокировать весь машинный трафик без оценки потери полезного поиска, доступности и партнёрских интеграций.

10. Требования к закупкам и подрядчикам

Ни один поставщик не видит всю картину. Площадка видит показы, средство защиты — запросы, система продаж — качество заявок, финансы — выручку. Договор должен соединять эти наблюдения и не позволять одному участнику одновременно определять проблему, измерять её и подтверждать собственный результат без независимой проверки.

Требование	Вопрос поставщику	Доказательство
Методика	Как определяется человек, полезная программа, вредоносная программа и неизвестное событие?	Описание признаков, частота пересмотра, ошибки первого и второго рода.
Прозрачность	Какие исходные события доступны заказчику?	Журналы, выгрузка, идентификаторы решений, срок хранения.
Независимость	Можно ли сопоставить результат с продажами и третьей стороной?	Интеграция и право независимой проверки.
Компенсация	Что происходит при подтверждённом недействительном трафике?	Срок, порядок возврата, предел ответственности.
Приватность	Какие данные устройства и поведения собираются?	Основание обработки, минимизация, срок удаления, местонахождение.
Полезные машины	Как не заблокировать поиск, доступность и разрешённых помощников?	Белые списки, подписи, правила объявления цели.

11. Вывод

> **Стратегическая позиция.** Компании не нужно доказывать, что интернет «мёртв». Достаточно признать, что необработанный цифровой сигнал больше не заслуживает автоматического доверия. Победит бизнес, который умеет подтверждать людей, происхождение данных и ответственность за содержимое, не разрушая удобство для честных клиентов и полезных машин.

Ближайший источник конкурентного преимущества — не очередной генератор содержимого, а способность измерять подтверждённое внимание, сохранять прямые отношения и превращать доверие в более низкую стоимость сделки. На горизонте до 2031 года это станет не отдельной программой безопасности, а базовой частью маркетинга, данных, продукта и корпоративного управления.

Приложение 1. Проверка спорных тезисов

Тезис из исследований	Оценка	Корректная формулировка
«Теория мёртвого интернета доказана»	Слишком сильно	Подтверждено доминирование машинных запросов в крупных измерительных контурах, но не исчезновение людей.
«57,4% всего интернета — боты»	Нужен знаменатель	Это оценка запросов в выбранном контуре Клаудфлэр; другие отчёты дают 51–53%.
«74,2% страниц созданы машиной»	Неточно	На 74,2% новых англоязычных страниц детектор Арефс нашёл признаки машинного содержимого; 2,5% классифицированы как полностью машинные.
«93% поиска не даёт перехода»	Контекстно верно	Оценка Семраш для раннего режима ответа с искусственным интеллектом на конкретной выборке 2025 года.
«Потери 250 млрд. долларов»	Оценка поставщика	В отрасли нет единой методики; для решения нужен диапазон и собственный аудит.
«84% обмена идёт в закрытых каналах»	Слабая актуальность	Направление миграции важно, но число нельзя считать текущей глобальной долей без свежей методики.
«Синтетические данные неизбежно разрушают модели»	Слишком сильно	Рекурсивная замена реальных данных создаёт риск; контролируемая смесь и сохранение реальных данных могут его снизить.
«Алгоритмы неизбежно поляризуют людей»	Не доказано	Крупный краткосрочный эксперимент показал ограниченный эффект; долгосрочные и контекстные риски требуют отдельного исследования.

Приложение 2. Русский словарь для руководителя

Используемый термин	Простое значение
Автоматический трафик	Запросы и действия, созданные программами без непосредственного клика человека.
Вредоносная автоматическая программа	Программа, которая крадёт, обманывает, перегружает, подбирает доступ или нарушает правила.
Оптимизация для систем ответов	Подготовка материала так, чтобы машинная система могла правильно понять, процитировать и связать его с брендом.

Используемый термин	Простое значение
Происхождение содержимого	Проверяемая история: кто создал файл, чем он изменялся и кто подписал результат.
Отравление данных	Намеренное или случайное добавление материалов, которые искажают аналитику или поведение модели.
Деградация модели	Потеря разнообразия и связи с реальностью при неконтролируемом обучении на результатах других моделей.
Подтверждённый человек	Участник, чьи признаки, история и контекст достаточны для конкретной операции без избыточного сбора личности.
Прямая аудитория	Люди, с которыми у компании есть собственный канал связи и согласие, а не только доступ через алгоритм площадки.

Ключевые проверенные источники

1. Отчёт Thales о вредоносных автоматических программах за 2026 год: Открыть источник
2. Cloudflare: экономика интернета автономных помощников: Открыть источник
3. Ahrefs: анализ 900 000 новых англоязычных страниц: Открыть источник
4. SparkToro: исследование поисков без перехода в 2026 году: Открыть источник
5. Semrush: ранняя статистика режима поиска с искусственным интеллектом: Открыть источник
6. Anthropic и партнёры: отравление модели малым числом документов: Открыть источник
7. Nature: деградация моделей при рекурсивном обучении на синтетических данных: Открыть источник
8. Труды Национальной академии наук: эксперимент о краткосрочной поляризации: Открыть источник
9. Европейская комиссия: статья 50 закона об искусственном интеллекте: Открыть источник
10. Европейская комиссия: сроки применения требований прозрачности: Открыть источник
11. Коалиция по происхождению цифрового содержимого: описание стандарта: Открыть источник
12. Глобальное исследование доверия к искусственному интеллекту, Кей-Пи-Эм-Джи и Мельбурнский университет: Открыть источник