МОШЕННИЧЕСТВО ПРИ ЦИФРОВОЙ ИДЕНТИФИКАЦИИ

Угрозы, масштабы, технологии противодействия и научный задел

Состояние на 2026 год.
Версия 2.0 | Редакция для внешнего распространения.

Закрытый фактологический, методологический и нормативный контур (сверено с первичными источниками).

Синтез ключевых выводов: эскалация угроз и технологический ответ

$442 млрд

Глобальные финансовые потери (оценка ИНТЕРПОЛ, 2025). Риск классифицирован как «высокий».

x4.5 раза

Прибыльность мошенничества с ИИ по сравнению с традиционными методами. Инструментарий доступен по минимальным ценам.

до 100%

Пропуск атак отдельными системами на независимых тестах DHS RIVTD. Необходим многослойный контур с доверенным захватом.

2026–2027

Синхронное вступление в силу требований EU AI Act, eIDAS 2.0 и 572-ФЗ. Регуляторное давление догоняет технологическое.

Доказательная база: классификация источников и степень доверия

[Уровень A]

Высший приоритет. Государственная статистика (FBI IC3, Банк России), нормативные акты (EU AI Act), технические тесты (DHS, NIST) и расследованные дела (Дело Arup). Макроориентиры и абсолютные бенчмарки.

[Уровень B]

Научный задел. Рецензируемые публикации (IEEE) и эталонные академические наборы.

[Уровни C/D]

Отраслевые данные. Отчеты вендоров (Entrust, LexisNexis). Показывают направление трендов (рост дипфейков, инъекций), но абсолютные цифры несопоставимы и не суммируются.

Паспорт метрики: Большинство цифр на рынке несопоставимы. Настоящий отчет строго фиксирует числитель, знаменатель и географию для каждого показателя.

Макроэкономика мошенничества: глобальные ориентиры

[A1]

Глобально: $442 млрд общих потерь от финансового мошенничества (ИНТЕРПОЛ).

[A1]

США: $893.3 млн — задокументированные потери исключительно от ИИ-мошенничества (FBI IC3, 2025). Рост синтетических личностей в кредитовании (оценка экспозиции $3.3 млрд).

[A1]

Великобритания: 72% всех записей в национальной базе Cifas связаны с мошенничеством с идентичностью и захватом счетов.

[A1]

Европейский союз: 4.2 млрд евро потерь (оценка ЕБА/ЕЦБ). Преступники смещаются к операциям, которые пользователь подтверждает сам.

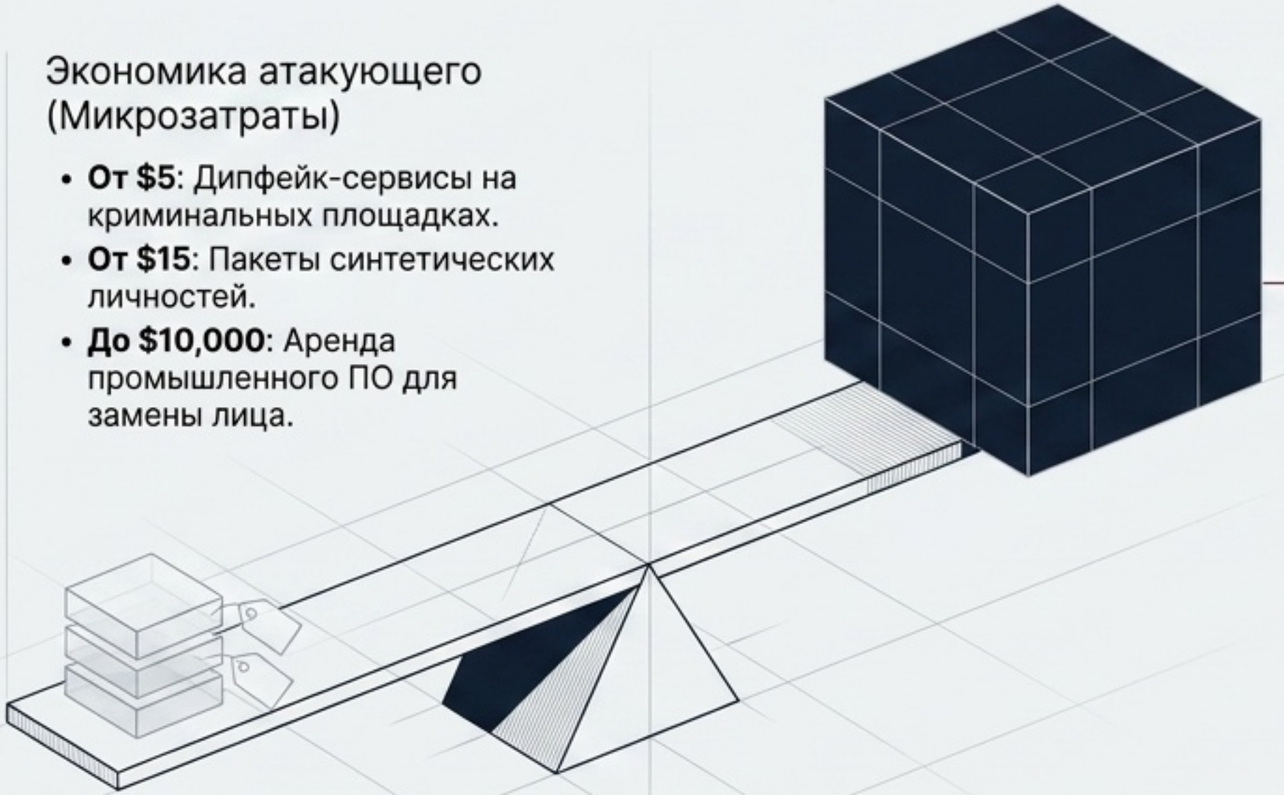
[A1]

Российская Федерация: 29.3 млрд руб. — объем операций без согласия клиентов (Банк России, 2025). Доля возврата снизилась до 5.9%.

Асимметрия угроз: кратное падение барьеров входа

Экономика атакующего (Микрозатраты)

- **От $5**: Дипфейк-сервисы на криминальных площадках.
- **От $15**: Пакеты синтетических личностей.
- **До $10,000**: Аренда промышленного ПО для замены лица.



[A4]

Масштаб ущерба (Макропотери)

Показательный инцидент [A4]: Дело Arup (Гонконг, 2024).

- **Ущерб:** ~$25.6 млн ($200 млн HKD).
- **Вектор:** Дипфейк финансового директора на видеоконференции, приведший к 15 авторизованным переводам.

Технологии генеративного ИИ снизили стоимость сложной атаки на порядки.
Доступность инструментария порождает массовый «агентный» трафик.

Анатомия угроз: смещение фокуса на захват действующих записей

Ключевой инсайт: Безопасная первичная регистрация аннулируется, если процедура восстановления доступа (например, через колл-центр или SMS) защищена слабее.

Крах однослойной защиты и ручного контроля

Человеческий фактор

[D] Только 0.1% людей безошибочно определяют современные дипфейки в тестовых сериях. При этом 57% сохраняют ложную уверенность в своих силах.

Вывод: Ручная визуальная проверка больше не может выступать основным барьером.

Государственные испытания DHS RIVTD [A3]

Худший сценарий:
Пропуск до 100% атак (APCER) у отдельных систем.

Лучшие системы:
Ошибка на атаках (APCER) <3.3% при ложных отказах (BPCER) <0.5%.

Вывод: Заявления вендоров о «99.3% точности» невалидны без независимых тестов. Качество систем на рынке варьируется радикально.

Архитектура доверия: 5-слойная модель противодействия

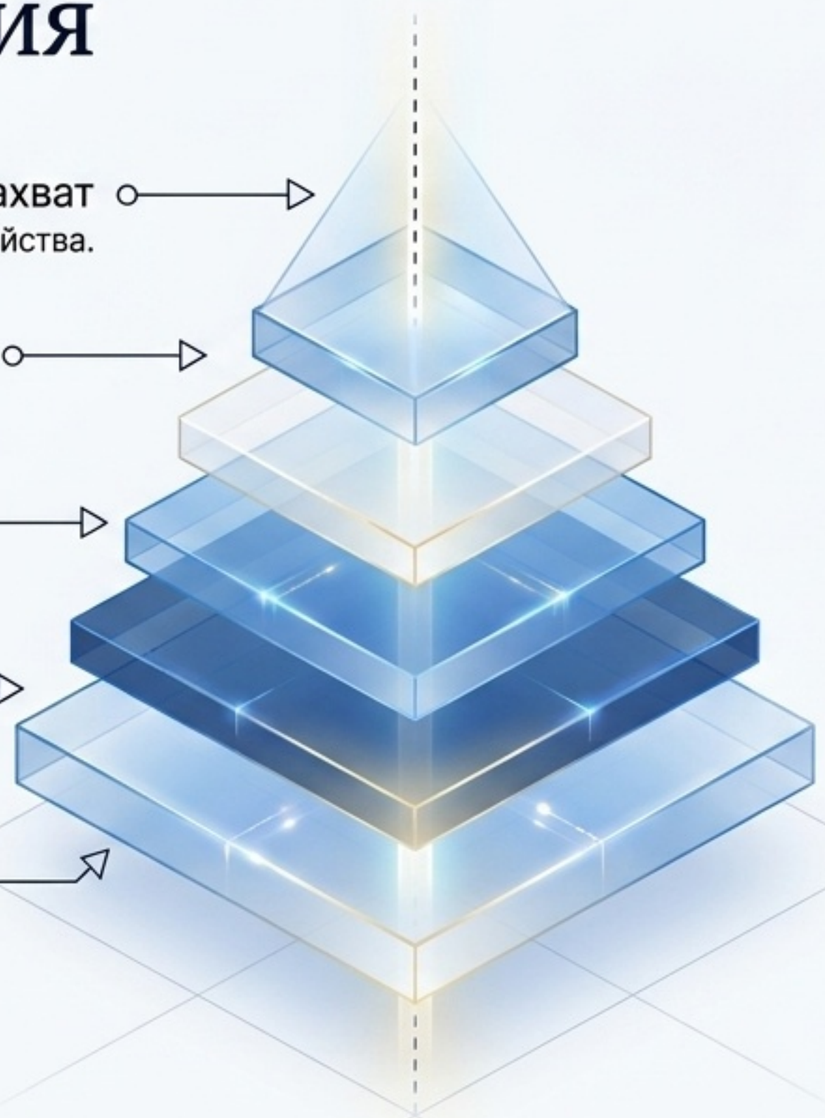
Слой 5: Сенсор и захват
Детекция инъекций, аттестация устройства.

Слой 4: Аналитика
Поведенческая биометрия, графовый анализ.

Слой 3: Процесс
Непрерывная переоценка риска сессии.

Слой 2: Сетевой уровень
Обмен сигналами, приватное сопоставление.

Слой 1: Инфраструктура доверия
Криптография, eIDAS, FIDO2.

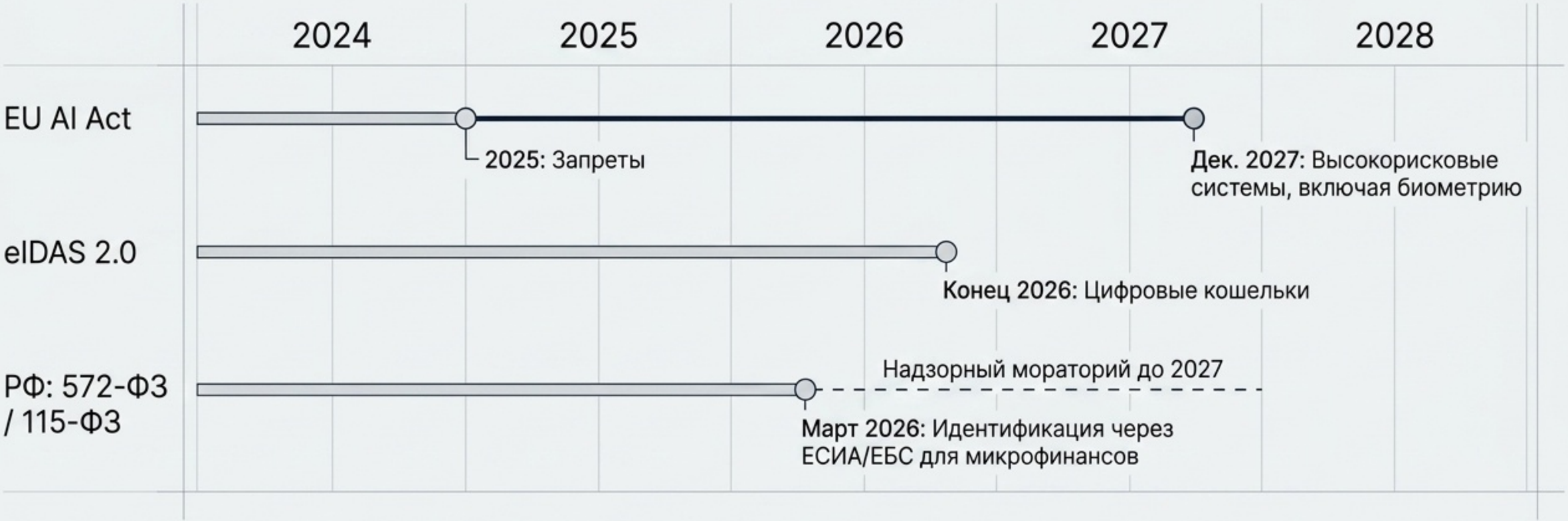


Сдвиг парадигмы: До 90% блокируемого мошенничества выявляется по сигналам мобильного SDK (доверие каналу захвата), а не по лицу.

Оценка решений: доказательная матрица вместо маркетинга

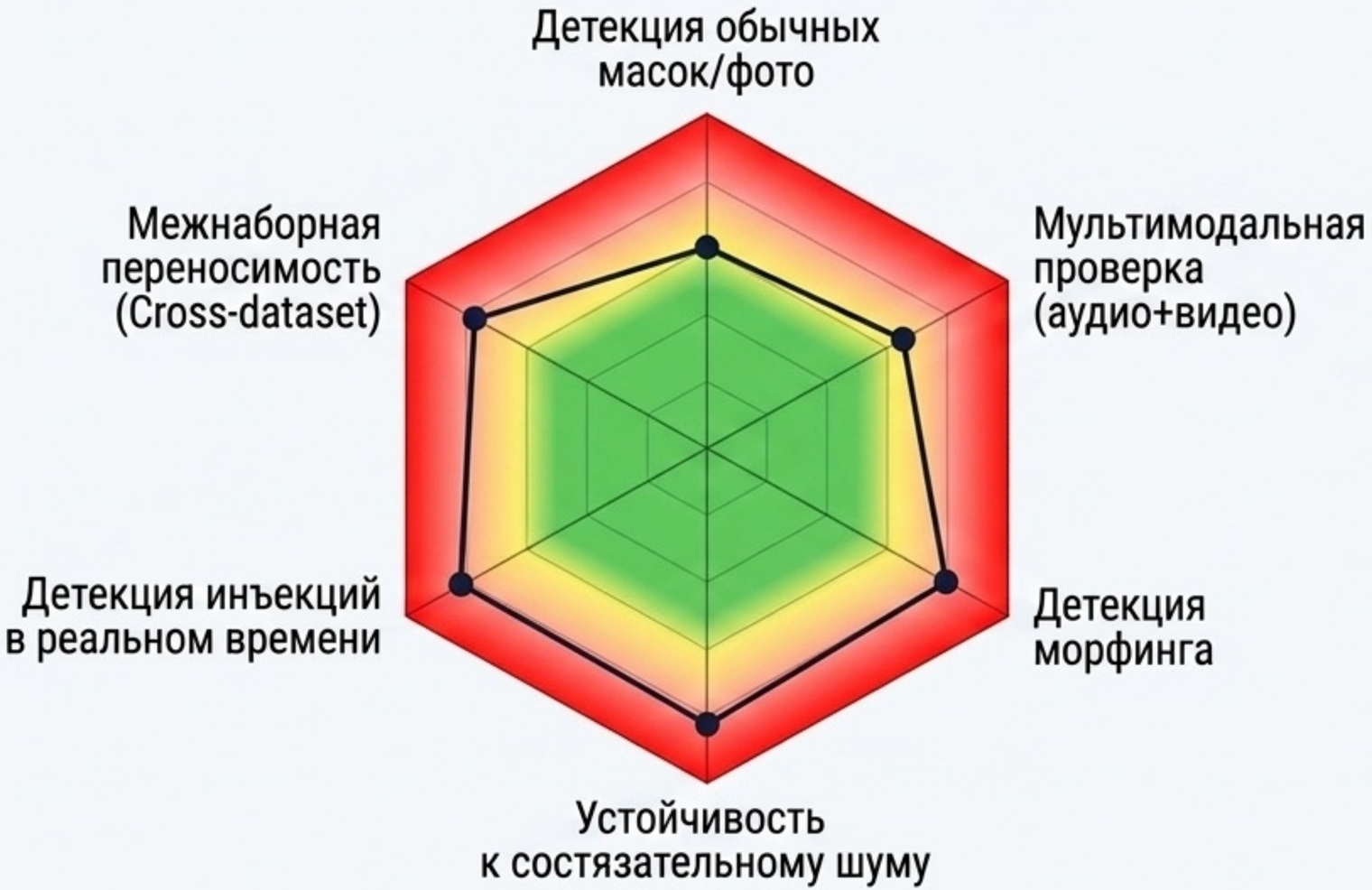
Критерий	Маркетинговые обещания ⚠️	Доказательные метрики ✅
Точность	«Точность 99%»	Раздельные метрики APCER (пропуск атак) и BPCER (отказ клиентам) в заявленной операционной точке.
Защита от атак	«Защита от дипфейков»	Отдельное тестирование презентационных атак (экраны) и инъекций потока (виртуальные камеры).
Сертификация	«Собственные тесты»	Отчеты NIST, DHS RIVTD/RIVR, iBeta (ISO/IEC 30107-3) с датой и версией.
Аудит и объяснимость	«ИИ черный ящик»	Журналирование причин отказа, доступность версии модели, прозрачный аудит.
Конфиденциальность	«Облачная обработка»	Строгие сроки хранения, отсутствие передачи исходных биометрических образцов третьим лицам.

Нормативный ландшафт: синхронизация требований (2024–2028) A2



Ключевой инсайт: Регуляторное давление нарастает синхронно с технологическим. Биометрия 1:1 исключена из высокого риска в ЕС, но скоринг с биометрией — требует толкования.

Научный горизонт: технологическая зрелость и слепые зоны [B]



Синтез:

Научный задел зрел против статичных презентационных атак, но систематически отстает против неизвестных ИИ-генераторов и цифровых инъекций.

Закупочные решения нельзя принимать только на базе академических тестов.

Триггеры приоритизации от собственных операционных данных

🔴 **Критический приоритет** (Немедленное реагирование)

- Успешная инъекция.
- Биометрия блокирует кредит без процедуры апелляции.
- Одно лицо в разных юрлицах группы.

🟡 **Высокий приоритет** (Требует архитектурных изменений)

- Восстановление доступа слабее регистрации.
- Мобильное приложение не использует аппаратную аттестацию (Play Integrity / App Attest).

⚪ Повышенный приоритет (Аналитический мониторинг)

- Растет число захватов счетов после успешной первичной проверки.
- Расхождение сигналов: документ подлинный, но интеллект устройства показывает аномалию.

Роадмап внедрения: этапный план перехода к нулевому доверию

Этап 1 (0-3 мес): Экстренные блокировки.

Внедрение детекции цифровых инъекций и аппаратной аттестации устройств. Запрос тестов DHS/iBeta у вендоров. Полный отказ от ручной визуальной проверки как основы.

Этап 2 (3-12 мес): Многослойный контур.

Интеграция 5-слойной защиты. Выравнивание уровня безопасности при восстановлении доступа с первичной регистрацией. Внедрение графового анализа сетевых связей.

Этап 2 (3-12 мес): Многослойный контур.

Этап 3 (12-24 мес): Непрерывный риск и комплаенс.

Переход к непрерывной переоценке риска на протяжении всей сессии. Крипто-удостоверения. Подготовка к EU AI Act.

Директива закупки: 6 обязательных вопросов поставщику

1. Паспорт метрик

Дайте полные данные (числитель, знаменатель, выборка) для заявленных маркетинговых процентов.

2. Государственные тесты

Покажите сертификаты DHS, NIST или iBeta (ISO/IEC 30107-3) именно на предлагаемую версию движка.

3. Худший сценарий

Раскройте максимальные (а не средние) метрики ошибок APCER и BPCER в разрезе типов атак.

4. Аудит ИИ

Опишите механизм предоставления причин отказа клиенту и возможности аудита версии модели.

5. Векторы инъекций

Предоставьте точный перечень обнаруживаемых векторов обхода камер и инъекций потока.

6. Комплаенс данных

Пропишите сроки хранения векторов, отсутствие трансграничной передачи и соответствие 572-ФЗ / GDPR.

Ограничения исследования и оговорки

- Природа данных вендоров: Отчеты поставщиков отражают специфику их сетей. Направления трендов подтверждаются, но абсолютные значения несопоставимы и не могут суммироваться.
- Оценочный характер сумм: Данные о глобальных потерях ($442 млрд) представляют собой институциональные макроориентиры, а не аудированные бухгалтерские суммы.
- Прогнозы как гипотезы: Экстраполяции роста потерь до 2030 года используются исключительно как сценарные гипотезы для стратегического планирования.
- Нормативный статус: Справки по EU AI Act, eIDAS 2.0 и 572-ФЗ представляют аналитический обзор первичных актов на август 2026 года и не заменяют профильного юридического заключения.