Мониторинг международных трендов правового регулирования для развития законодательства в сфере цифровой экономики в России

- Новые обязанности платформ по борьбе с мошенниками
- Международная практика защиты данных при парсинге

Мониторинг №10 (34) (Октябрь 2026)

Мониторинг подготовлен коллективом сотрудников лаборатории анализа лучших международных практик Института Гайдара.
Авторский коллектив: науч. сотр. Гирич М.Г., науч. сотр. Ермохин И.С., ст. науч. сотр. Левашенко А.Д., науч. сотр. Солдаткина О.С., науч. сотр. Черновол К.А., науч. сотр. Синельникова-Мурылева Д.А.

При частичном или полном использовании материалов ссылка на источник обязательна

Кругом обман!

Новые обязанности платформ по борьбе с мошенниками

Автор: Кирилл Черновол

Мошеннические схемы часто эволюционируют одновременно с технологиями. И регуляторы стали возлагать обязанности по борьбе с мошенниками на платформы.

ЕС в октябре 2026 г. опубликовал исследование о 6 видах схем в финансовой сфере, связанных с инвестициями, знакомствами, электронной коммерцией, легким заработком, трудоустройством и благотворительностью.

На маркетплейсах создаются фальшивые карточки товаров или продавцов, а при помощи ИИ таких карточек можно сделать больше, чем человек способен «отсеять». Покупатель заходит в такую карточку, например, на классифайде (как Авито), общается с ИИ-чатботом, который выдает себя за продавца, переводит деньги за товар или услугу, после чего мошенник пропадает.

Для борьбы с такими практиками в октябре 2026 г. Еврокомиссия начала расследование в отношении Booking.com, чтобы оценить эффективность мер платформы по снижению рисков размещения поддельных объявлений о жилье, рисков неправомерного использования данных о гостях и бронированиях. Еврокомиссия проверяет порядок передачи данных гостиницам и работу переписки внутри Booking.

3,2 млн $

в среднем похищают мошенники в блокчейн-сетях за одну операцию с использованием ИИ

Еще пример – сайты знакомств и соцсети. Здесь мошенники выманивают деньги и платежные данные у жертв под видом онлайн-отношений, романтической переписки или секстинга. Такую переписку могут вести ИИ-чатботы. Другая схема - выдавать себя за знакомого жертвы и просить деньги якобы на помощь. Кстати, минимум в 5 странах мира секстинг запрещен или ограничен законом[1], а в Китае такой запрет установлен именно для генеративного ИИ.

В этом контексте в США в октябре 2026 г. приняли закон, обязывающий платформы для знакомств уведомлять пользователей о контактах с мошенниками. Если сервис блокирует аккаунт мошенника, он должен предупредить всех пользователей, получавших от этого аккаунта сообщения.

Дипфейки. Мошенники имитируют лицо и голос, например, топ-менеджера компании, чтобы убедить жертву – работника компании перевести им деньги. Так, в 2024 г. сотрудник подразделения британской компании Arupa в Гонконге получил письмо якобы от финансового директора головного офиса с поручением провести конфиденциальную операцию. Затем его пригласили на видеоконференцию, где «финансовый директор» и другие «коллеги», чьи изображения и голоса были подделаны ИИ, убедили его перевести им около 25,6 млн долл. Поймали ли мошенников, неизвестно.

Атаковать преступники могут не только людей, но и ИИ-агентов. Еврокомиссия указывает на угрозу атак на ИИ при помощи «промпт-инъекций». Дело в том, что ИИ, анализируя тексты, не всегда отличает информацию, которую должен обработать, от команд, которые должен выполнить. Например, просматривая для пользователя сообщения в соцсетях, ИИ может обнаружить в одном из них скрытую инструкцию («промпт») и принять ее за команду пользователя, например, передать чувствительные данные или перевести деньги на счет злоумышленника.

Так, в июне 2026 г. в открытом хранилище GitHub был обнаружен код для облачной платформы Microsoft Azure, который якобы должен был помогать пользователям настраивать их проекты на этой платформе. Но документация проекта содержала инструкцию для ИИ-агента

[1] Нигерия, Оман, ОАЭ, Индия, Бангладеш.

Cursor - собрать и передать мошенникам ключи доступа пользователей ко всевозможным сервисам (GitHub, облачным платформам AWS, Azure, Google Cloud и др.). Всего под атаку попали 73 хранилища Microsoft.

Бороться с такими практиками Еврокомиссия рекомендует путем проверок участников платформ (продавцов, рекламодателей, исполнителей и т.д.), выявления ключевых слов в переписках, создания систем жалоб на мошеннические действия. Предлагается развивать обмен сведениями о мошенниках между платформами, банками, операторами связи и правоохранительными органами. Для пользователей - предусматривать предупреждения о возможном мошенничестве до передачи денег, дополнительные подтверждения и «периоды охлаждения», когда деньги по подозрительной операции можно перевести только спустя какое-то время, чтобы у жертвы была возможность обратиться за помощью.

В России, согласно Федеральному закону «О платформенной экономике», операторы посреднических цифровых платформ обязаны проверять партнеров – продавцов, исполнителей и т.д. через государственные реестры, а также проверять информацию в карточках товаров (как сведения о разрешительных документах, маркировках). Для взаимодействия государственных органов, банков, операторов связи и мессенджеров в России действует ГИС «Антифрод», которая помогает получать информацию об известных мошенниках и вовремя блокировать их деятельность. С марта 2027 г. к этой системе обязаны будут подключаться и маркетплейсы.

А что дальше?

В России уже внедрены общие нормы по борьбе с мошенничеством на платформах. Нет специального регулирования для мошенничества с использованием ИИ.

Во сколько обойдется маркетплейсам обеспечение безопасности сделок от мошенников? По данным Data Insight, в 2026 г. количество онлайн-заказов на маркетплейсах в России составит около **8,1** млрд, т.е. его рост с 2025 г. составит **20%**. Такими темпами, даже если проверка 1 заказа будет стоить 1 руб., в 2027-2030 гг. маркетплейсы должны будут потратить **52,18** млрд руб. на борьбу с мошенниками[1].

Впрочем, цена ущерба куда больше: по данным Банка России, сумма переводов клиентов злоумышленникам в 2024 г. составила **26,86** млрд руб., а в 2025 г. – **28,25** млрд руб. Таким образом, за 2027-2030 гг. мошенники могут получить с россиян минимум **135** млрд руб.[2]

[1] Если количество заказов на российских маркетплейсах растет на 20% ежегодно, а одна проверка каждого заказа обходится в 1 руб., то 8,1 млрд руб. в 2026 г. * 1,2 за каждый следующий год, получаем 9,72 млрд руб. в 2027 г., 11,66 млрд руб. в 2028 г., 14,00 млрд руб. в 2029 г. и 16,80 млрд руб. в 2030 г. Всего за 2027–2030 гг. - 52,18 млрд руб.

[2] Если сумма зарегистрированных банками хищений у физических лиц растет на 5,16% ежегодно, как между 2024 и 2025 гг., то расчетные 29,71 млрд руб. в 2026 г. * 1,0516 за каждый следующий год, получаем 31,24 млрд руб. в 2027 г., 32,86 млрд руб. в 2028 г., 34,55 млрд руб. в 2029 г. и 36,33 млрд руб. в 2030 г. Всего за 2027–2030 гг. - 134,99 млрд руб.



Борьба с мошенничеством через блокировку мошеннических сайтов и контроль подозрительных платежей, защиту персональных и платежных данных

Возложение обязанностей на платформы по предупреждению мошенничества до причинения ущерба

Расширение обязанностей платформ: ужесточение требований по проверке подлинности личности пользователей на платформах, усиление контроля платформ за доступом ИИ-агентов к данным и деньгам: защита от «промпт-инъекций», дополнительное подтверждение переводов, действий человека и пр.

Безопасный парсинг данных: все или ничего

Международная практика защиты данных при парсинге

Авторы: Ольга Солдаткина

Парсинг данных (или веб-скрапинг - автоматизированный сбор данных с веб-страниц) не только подбрасывает «топливо» (данные) в гонку ИИ-технологий, но и бросает вызов конфиденциальности персональных данных. Традиционно защита данных строилась на обеспечении контроля субъекта над своими данными, получения компаниями согласия пользователя на использование его данных. Но как можно контролировать использование данных, если их собирает неподконтрольный для человека ИИ?

В октябре 2026 г. ОЭСР представила доклад по повышению пользовательского контроля в контексте ИИ. ОЭСР отмечает, что ИИ-боты чаще собирают данные не для обучения, а для ответа на разовый запрос пользователя (технология RAG – генерация с дополненной выборкой), поэтому настройки для парсинга неприменимы. В связи с этим южнокорейская Комиссия по защите персональных данных рекомендует фильтровать данные как при сборе, так и при выдаче результата моделью, когда ИИ обращается к внешним базам через RAG.

ОЭСР рекомендует работать с ИИ-рисками на нескольких уровнях.

На уровне регуляторов необходимы разъяснения, как применять действующие требования к данным. Например, в ЕС целевая группа EDPB по ChatGPT разъясняет, как трактовать GDPR[1] в контексте применения больших языковых моделей. Главный вывод – разработчик не может перекладывать ответственность на пользователя модели через пользовательские соглашения, например, предупреждением не вводить в чат чувствительные данные о здоровье.

На уровне источников данных (на сайтах), например, могут устанавливаться запреты на автоматизированный сбор данных, а также внедряться технические барьеры, такие как применение файлов «robots.txt» (стандарт, с помощью которого сайт сообщает поисковым роботам, какие разделы им можно посещать) или функции Cloudflare (блокировка ИИ-ботов на сетевом уровне одной настройкой).

17% *сайтов уже поставили ограничения на парсинг данных для обучения, по оценкам Cloudfare*

На уровне разработчиков также могут применяться инструменты контроля данных. Например, многоступенчатая фильтрация позволяет разработчикам отсеивать персональные и чувствительные данные до момента их включения в обучающий набор данных. Могут применяться и техники отслеживания происхождения данных, когда к каждому фрагменту информации прикрепляется метка, с какого сайта он собран. Например, французский регулятор по защите данных CNIL представил инструмент отслеживания источников данных, выдаваемых ИИ, - техника позволяет при необходимости изымать фрагменты данных из готового датасета (набора данных) для обучения ИИ.

Важно также поддерживать прозрачность самой работы данных: в собираемых наборах данных указывать источники сбора, критерии исключения и методы фильтрации.

В контексте парсинга нужно сместить фокус с защиты данных от нарушений (о свершении которых человек может никогда и не узнать) к добросовестному обращению с данными при работе с ИИ. Так, в октябре в ЕС обсуждалось Руководство по веб-скрапингу для генеративного ИИ в части применения GDPR при парсинге. В основе безопасного парсинга лежит принцип «не видеть больше пользователя», т.е. не

1 GDPR (General Data Protection Regulation) - Общий регламент ЕС по защите персональных данных 2016 г.

собирать данные, которые не видит сам пользователь на сайте, но различает ИИ-парсер.

Публикация данных в открытом доступе не означает согласия на их парсинг. Но поскольку при масштабном скрапинге индивидуальное согласие получить трудно, разработчик может собирать данные без согласия, если это нужно для понятной и законной цели (например, обучения модели) – такое основание обработки известно как «законный интерес».

На первый взгляд, парсинг данных и минимизация сбора данных – это взаимоисключающие вещи. Но при парсинге принцип минимизации начинает применяться еще до сбора данных, когда разработчик определяет критерии фильтрации данных. Более того, «отбраковывание» данных проводится и на этапе формирования обучающего датасета, т.е. минимизация данных, используемых для ИИ, происходит и после парсинга. Принцип минимизации указывает не на объем данных, а на порядок их отбора.

В России законность парсинга основывается на нормах об общедоступной информации. Однако решение суда в деле «ВКонтакте против Дабл» (2021 г.) показало, что, хотя данные пользователей ВКонтакте доступны публично, их парсинг для подготовки аналитических продуктов и коммерческой реализации нарушает права ВКонтакте на базу данных.

Эпоха ИИ меняет наше представление не только о способах сбора данных, но и о самих категориях данных, с которыми можно работать. Например, нейроданные, т.е. данные о работе нервной системы человека. С одной стороны, данные о физиологическом и ментальном состоянии человека относятся к данным о здоровье, т.е. к персональным. С другой стороны, можно ли считать персональными данными машинные интерпретации или вычисления сигналов нервной системы (так называемые «inferred data» - выведенные данные)? Ведь здесь размывается граница между тем, что производит человек (его нервная система) и что фиксируют технологии в качестве данных о нем (о его нервной системе). В докладе об управлении нейроданными аналитики ОЭСР отмечают необходимость адаптации регулирования данных под новый тип ИИ – фундаментальные модели мозга (Brain Foundation Models), которые основаны на анализе нейросигналов. Причем выведенные данные могут оказаться чувствительнее исходных. Однако выводы ИИ об эмоциях, намерениях и когнитивных паттернах могут выпасть из-под защиты законодательства о данных, притом что такие данные не менее чувствительны, чем данные о здоровье, и поэтому могут требовать сопоставимого уровня защиты.

А что дальше?

Пока правила обсуждаются, данные россиян уже собираются. В глобальном веб-архиве Common Crawl русский язык - второй язык после английского по объему данных, которые можно парсить для обучения ИИ. Из 160 идентифицированных языков на русский язык приходится **6,3%** веб-страниц (**136,1 млн** страниц). Но даже такой запас не бесконечен. По оценке Epoch AI, всего в открытом доступе порядка **300 трлн текстов**, созданных людьми и пригодных для обучения ИИ. С вероятностью **80%** модели полностью исчерпают этот запас между 2026 и 2032 г. Это значит, что следующие поколения ИИ будут все чаще обучаться не на данных, созданных человеком, а на генерациях предыдущих моделей ИИ.


ВЧЕРА
СЕГОДНЯ
ЗАВТРА
2006-2026 гг.
Россия, ЕС
октябрь 2026 г.
страны ОЭСР, ЕС разрабатывают стандарты защиты данных при парсинге
Нормы об общедоступных данных допускали парсинг в отношении данных в отрытом доступе
Стали вводиться стандарты по ограничению парсинга даже в отношении публично доступных данных, такие как отфильтровка чувствительных данных
Расширение требований по парсингу для ИИ не только в отношении парсеров, но и самих источников данных, как требование применить блокаторы для считывания данных

Новости **в октябре 2026 г.**, которые показались нам интересными[1].

- В США предложено запретить крупным продуктовым магазинам и их онлайн-платформам устанавливать индивидуальные цены на основе персональных данных покупателей (возраста, дохода и др.), использовать биометрию для ценообразования, а также повышать цены в зависимости от предполагаемого времени покупок.

- В ЕС предложили увеличить в **50** раз (с 6 млрд до 300 млрд евро) лимит стоимости токенизированных акций и облигаций, которыми могут торговать блокчейн-площадки, а также допустить к таким торгам криптобиржи с лицензией по MiCA (Регламенту ЕС о рынках криптоактивов).

- В США предложено упростить привлечение финансирования через выпуск криптоактивов (ICO): освободить компании от обязательной регистрации по законодательству о ценных бумагах при привлечении до **5** млн долл. за 4 года или до **75** млн долл. в год при соблюдении дополнительных требований к отчетности.

- В России Центробанк определил правила бухгалтерского учета цифровой валюты для банков: снижение ее стоимости необходимо отражать как убыток, даже если валюта еще не продана, а прибыль от роста стоимости - только после продажи. Например, если банк купил цифровую валюту за 1 млн руб., а ее стоимость снизилась до 800 тыс. руб., он должен отразить убыток в 200 тыс. руб. Если же стоимость вырастет до 1,2 млн руб., прибыль в 200 тыс. руб. можно будет учесть только после продажи. Такой подход уже применяется в бухгалтерском учете товаров.

- Минцифры предложило меры борьбы с ИКТ-преступлениями: граждане смогут через Госуслуги проверять, кому дали согласие на обработку персональных данных, и отзывать его. При этом перечень собираемых данных и цели их обработки будут определять профильные министерства.

- В Норвегии планируют ограничить использование умных очков с ИИ в общественных местах (парках, пляжах, музеях, школах и др.) для предотвращения съемки людей без их согласия.

- Роскомнадзор подхватил тренд на ограничение использования детьми соцсетей - предложил ввести обязательную идентификацию детей в соцсетях и ограничить время пребывания в интернете детей до 14 лет.

[1] С 2025 г. Институт Гайдара разрабатывает цифровую платформу анализа новостей в России и в мире по тематике регулирования цифровой экономики – DIgiReg. Представленные новости отобраны экспертами в том числе на основе анализа данных платформ.