Кризис цифрового доверия в эпоху генеративного искусственного интеллекта: предпосылки развития механизмов проверки информации и профилактики цифрового мошенничества

Автор: Величко Екатерина Вадимовна

Аффилиация: независимый исследователь в области цифровой грамотности, искусственного интеллекта и цифровой безопасности, Россия.

Аннотация

В статье рассматривается проблема цифрового доверия в условиях массового распространения генеративного искусственного интеллекта и трансформации цифровых мошеннических сценариев. На основе открытых статистических и аналитических данных МВД России, Банка России, ВЦИОМ и ИСИЭЗ НИУ ВШЭ анализируется динамика цифровых рисков в России в 2023–2026 годах. Показано, что после роста преступлений, совершённых с использованием информационно-телекоммуникационных технологий, в 2023–2024 годах в 2025 году и начале 2026 года зафиксировано снижение ряда показателей. Данная тенденция свидетельствует об усилении государственного, межведомственного и финансового противодействия цифровой преступности.

Одновременно данные Банка России указывают на сохранение значимого финансового ущерба, рост количества операций без добровольного согласия клиентов и усложнение мошеннических схем, основанных на социальной инженерии, фишинговых ссылках, вредоносном программном обеспечении и комбинированных сценариях воздействия на пользователя. Отдельное внимание уделяется массовому использованию нейросетей в России: по данным ВЦИОМ, каждый второй интернет-пользователь обращался к нейросетям в течение года, а среди наиболее частых целей названы поиск информации, консультации, создание текстов и анализ данных.

В статье обосновывается, что цифровая безопасность в эпоху генеративного ИИ должна рассматриваться не только как техническая защита от вредоносных ресурсов, но и как система оценки цифрового доверия. Такая система включает проверку информации, источников, контекста, цифровых сообщений, документов и последствий пользовательского действия. Делается вывод о необходимости развития механизмов проверки информации и профилактики цифрового мошенничества, ориентированных на принцип «проверить до действия».

Введение

Искусственный интеллект как область научных исследований и технологических разработок существует несколько десятилетий. Однако именно 2022–2023 годы стали периодом резкого роста общественного интереса к генеративным моделям и их массового распространения среди непрофессиональных пользователей. Нейросетевые инструменты начали использоваться не только специалистами в области информационных технологий, но и широкими группами граждан: для поиска информации, подготовки текстов, анализа данных, создания изображений, перевода, обучения, работы и бытовых решений.

Для России этот процесс совпал с более широким изменением цифрового поведения населения: ростом дистанционных финансовых операций, использованием мессенджеров, онлайн-банкинга, маркетплейсов, электронных государственных услуг и удалённых форм коммуникации. В такой среде человек всё чаще принимает решения на основе цифрового объекта: сообщения, ссылки, файла, документа, ответа нейросети, изображения, аудио- или видеоматериала.

Проблема состоит не в самом факте развития ИИ. Генеративные модели создают значимый потенциал для экономики, образования, науки, бизнеса и повседневной продуктивности. Проблема заключается в разрыве между скоростью внедрения цифровых инструментов и уровнем готовности пользователя к их безопасному применению.

С одной стороны, пользователь получает быстрый доступ к информации и автоматизации. С другой стороны, он сталкивается с новыми рисками: ошибочными ответами ИИ, неподтверждёнными фактами, фишинговыми

ссылками, поддельными документами, мошенническими сообщениями, манипулятивными сценариями и синтетическим контентом. В результате формируется кризис цифрового доверия: пользователю всё сложнее определить, чему можно доверять, что необходимо перепроверить и какие действия могут привести к финансовому, юридическому, репутационному или информационному ущербу.

Цель настоящей статьи: проанализировать предпосылки кризиса цифрового доверия в России в 2023–2026 годах и обосновать необходимость развития механизмов проверки информации, цифровых сообщений, документов и пользовательских действий в условиях массового применения генеративного ИИ.

Материалы и методы

Исследование выполнено в формате обзорно-аналитической работы. В качестве эмпирической базы использованы открытые официальные и аналитические источники:

- статистические сведения МВД России о состоянии преступности за 2023, 2024, 2025 годы и январь–февраль 2026 года;
- обзоры Банка России об операциях, совершённых без согласия или без добровольного согласия клиентов финансовых организаций, за 2023–2025 годы;
- данные ВЦИОМ о восприятии и использовании нейросетей интернет-пользователями в России;
- данные ИСИЭЗ НИУ ВШЭ, основанные на обследованиях Росстата по применению искусственного интеллекта в организациях;
- нормативные и методические материалы, связанные с оформлением научных публикаций и библиографических ссылок.

Методологически работа опирается на:

1. сравнительный анализ статистических данных за 2023–2026 годы;
2. содержательный анализ цифровых рисков;
3. классификацию пользовательских угроз;
4. интерпретацию статистики с учётом различий методологии МВД России и Банка России;

5. обобщение предпосылок для развития механизмов цифровой проверки.

Исследование не включает сбор персональных данных, медицинские вмешательства, психологические эксперименты, опросы респондентов или работу с уязвимыми группами. Поэтому одобрение комитета по научной этике и получение информированного согласия участников исследования не требуется.

Массовое использование нейросетей как фактор изменения цифрового поведения

Данные ВЦИОМ показывают, что нейросети уже стали заметной частью цифрового поведения россиян. В октябре 2025 года ВЦИОМ сообщил, что каждый второй российский интернет-пользователь обращался к нейросетям в течение последнего года, а самой популярной целью их применения был поиск информации — 63%. Среди наиболее узнаваемых инструментов были названы ChatGPT, YandexGPT, DeepSeek, GigaChat и «Шедеврум».

В декабре 2025 года ВЦИОМ также сообщил, что 92% интернет-активных россиян декларируют интерес к теме ИИ. Среди наиболее распространённых задач использования нейросетей были названы консультации и поиск советов, развлечения, создание текстов, переводы, создание изображений и графики, обработка фото и видео, анализ больших объёмов информации.

Эти данные важны по двум причинам.

Во-первых, нейросети используются не только для развлечения. Они становятся инструментом поиска информации, подготовки текстов, консультаций и анализа. Следовательно, результат работы ИИ может влиять на реальные действия пользователя: подготовку документов, деловую переписку, публикацию материалов, принятие решений, поиск правовой, финансовой или медицинской информации.

Во-вторых, высокий уровень использования не равен высокому уровню понимания ограничений технологии. Нейросеть может создавать убедительный текст, но убедительность формы не гарантирует

достоверность содержания. Пользователь, не обладающий навыками проверки источников, может принять вероятностно сгенерированный ответ за подтверждённый факт.

Поэтому массовое распространение нейросетей усиливает потребность не только в цифровой грамотности в классическом смысле, но и в новой компетенции — оценке цифрового доверия. Эта компетенция включает умение проверять источник, контекст, достоверность, риск действия и возможные последствия ошибки.

Динамика преступлений с использованием ИКТ в России: 2023–2026 годы

Статистика МВД России показывает, что в 2023–2024 годах преступления, совершённые с использованием информационно-телекоммуникационных технологий, стали одной из ключевых составляющих общей структуры преступности.

В 2023 году, по данным МВД России, каждое третье преступление было совершено с использованием информационно-телекоммуникационных технологий. Количество таких деяний выросло на 29,7% по сравнению с 2022 годом.

В 2024 году доля таких преступлений достигла 40% от всех зарегистрированных преступлений. МВД также указало, что их количество увеличилось на 13,1% по сравнению с 2023 годом, а тяжких и особо тяжких составов — на 7,8%.

В 2025 году динамика изменилась. МВД России сообщило, что по итогам года преступлений, совершённых с использованием информационно-телекоммуникационных технологий, было зарегистрировано на 11,8% меньше, чем в 2024 году. Количество дистанционных краж снизилось на 23,6%, дистанционных мошенничеств — на 9%, а преступлений в сфере компьютерной информации — на 42,2%.

За январь–февраль 2026 года снижение продолжилось: МВД зафиксировало на 29% меньше преступлений, совершённых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, по сравнению с январём–февралём

2025 года. При этом количество преступлений в сфере компьютерной информации снизилось на 50,7%, дистанционных краж — на 18,8%, ИТТ-мошенничеств — на 21,3%.

Таблица 1. Динамика преступлений с использованием ИКТ по данным МВД России

Период	Ключевой показатель	Значение	Интерпретация
2023 год	Доля преступлений с использованием ИКТ	Каждое третье преступление	Цифровые каналы стали значимой частью преступности
2023 год	Рост ИКТ-преступлений к 2022 году	+29,7%	Зафиксирован резкий рост цифрового криминального воздействия
2024 год	Доля преступлений с использованием ИКТ	40%	Цифровые преступления стали системным фактором общей преступности
2024 год	Рост ИКТ-преступлений к 2023 году	+13,1%	Рост продолжился, но темп ниже, чем в 2023 году
2025 год	Преступления с использованием ИКТ к 2024 году	−11,8%	Зафиксировано снижение после периода роста
2025 год	Дистанционные мошенничества	−9%	Снижение не отменяет сохранение риска
Январь–февраль 2026 года	Преступления в сфере компьютерной информации	−29% к январю–февралю 2025 года	Тенденция снижения продолжилась в начале 2026 года

Данная динамика требует аккуратной интерпретации. Снижение отдельных показателей не означает исчезновения цифровых рисков. Оно

может отражать результат усиления государственного противодействия, профилактики, антифрод-механизмов, законодательных изменений и межведомственного взаимодействия. При этом сама структура риска остаётся значимой: цифровая среда стала одним из ключевых каналов воздействия на пользователя.

Финансовое мошенничество и операции без добровольного согласия клиентов

Данные Банка России показывают более сложную картину. Даже при снижении ряда уголовных показателей сохраняются финансовые потери и высокая активность мошеннических операций.

В 2023 году объём операций без согласия клиентов увеличился по сравнению с 2022 годом на 11,48%. Банк России также сообщил, что кредитные организации предотвратили 34,77 млн мошеннических операций на сумму 5 798,35 млрд рублей. Кроме того, Банк России направил операторам связи 575 669 телефонных номеров, используемых злоумышленниками для хищения средств у граждан.

В 2024 году объём операций без добровольного согласия клиентов увеличился по сравнению с 2023 годом на 74,36%. С 25 июля 2024 года начало действовать обновлённое регулирование, уточнившее определение операции без добровольного согласия клиента как денежного перевода, совершённого вследствие обмана или злоупотребления доверием.

В 2025 году объём операций без добровольного согласия клиентов увеличился по сравнению с 2024 годом на 6,4%, а их количество — на 31,2%. Банк России также указал, что с 1 октября 2025 года в мобильных приложениях крупных банков стало обязательным наличие специального сервиса для пострадавших, позволяющего оперативно заявить об операции без добровольного согласия и получить электронную справку для обращения в полицию.

Особое значение имеет качественное описание мошеннических сценариев. В 2025 году Банк России указал, что злоумышленники, используя приёмы и методы социальной инженерии, зачастую убеждали человека не просто самостоятельно совершить операцию, а перейти по фишинговой ссылке или скачать вредоносное программное обеспечение.

Это позволяло получить удалённый доступ к дистанционному банковскому обслуживанию или реализовать сценарии передачи данных платёжной карты.

Таблица 2. Динамика операций без согласия / без добровольного согласия клиентов по данным Банка России

Период	Показатель	Значение	Интерпретация
2023 год	Объём операций без согласия клиентов к 2022 году	+11,48%	Финансовый ущерб продолжил расти
2023 год	Предотвращённые мошеннические операции	34,77 млн операций	Антифрод-системы банков предотвратили значительный объём хищений
2023 год	Объём предотвращённых операций	5 798,35 млрд руб.	Масштаб предотвращённых угроз значительно превышает фактический ущерб
2024 год	Объём операций без добровольного согласия клиентов к 2023 году	+74,36%	Зафиксирован резкий рост объёма таких операций
2025 год	Объём операций без добровольного согласия клиентов к 2024 году	+6,4%	Рост замедлился, но не прекратился
2025 год	Количество операций без добровольного согласия клиентов	+31,2%	Количество фиксируемых эпизодов увеличилось
2025 год	Средняя сумма одной операции	18,6 тыс. руб.	Средний размер снизился, но массовость эпизодов выросла

Таким образом, финансовая статистика показывает не только количественный риск, но и важный качественный сдвиг: пользователь становится центральной точкой атаки. Техническая защита банков усиливается, но мошенническая коммуникация всё чаще направлена на то, чтобы сам человек совершил действие: перешёл по ссылке, ввёл данные, скачал приложение, поверил сообщению, подтвердил операцию или передал код.

Противоречие статистики: снижение ИКТ-преступности и сохранение цифрового риска

На первый взгляд, данные МВД России за 2025 год и начало 2026 года могут создавать впечатление, что проблема цифрового мошенничества снижается и теряет актуальность. Однако сопоставление с данными Банка России показывает более сложную структуру.

С одной стороны, правоохранительная статистика фиксирует снижение числа зарегистрированных преступлений с использованием ИКТ. С другой стороны, финансовая статистика показывает рост количества операций без добровольного согласия клиентов и сохранение многомиллиардных потерь.

Это противоречие не является ошибкой. Оно объясняется различиями в методологии учёта:

- МВД фиксирует преступления в уголовно-правовой логике;
- Банк России фиксирует операции без добровольного согласия клиентов финансовых организаций;
- часть пострадавших может обращаться только в банк, но не в полицию;
- часть случаев может не квалифицироваться как преступление на момент первичной фиксации;
- изменения в инструментах подачи заявлений могут повышать регистрируемость операций;
- усиление антифрод-систем может снижать крупные потери, но увеличивать фиксацию малых эпизодов.

Для темы цифрового доверия это означает следующее: оценивать проблему только по одному показателю неправильно. Необходимо

анализировать одновременно преступность, финансовые операции, поведенческие сценарии, уровень цифровой грамотности и массовое использование ИИ.

Искусственный интеллект в организациях: внедрение растёт, компетенции ограничены

По данным ИСИЭЗ НИУ ВШЭ, основанным на обследовании свыше 15 тыс. крупных и средних организаций — пользователей ИИ, проведённом Росстатом в 2025 году, технологии искусственного интеллекта уже применялись в различных отраслях экономики и социальной сферы. Наиболее востребованными оказались обработка визуальных данных, обработка текста, обработка звуковых данных, интеллектуальная поддержка принятия решений и технологии повышения эффективности ИИ.

При этом численность работников с компетенциями в области ИИ по итогам 2024 года превысила 242 тыс. человек, что составляло менее 1% численности работников списочного состава обследованных организаций. Из них 39 тыс. были специалистами по ИИ, а 203 тыс. — сотрудниками, использующими ИИ для решения профессиональных задач.

В 2026 году ИСИЭЗ НИУ ВШЭ также указал, что средняя доля организаций, использующих технологии ИИ, составляет 4,8%. При этом в организациях с численностью более 500 человек показатель достигает 14,9%, а в организациях с численностью 100 и менее человек — 4,1%.

Эти данные позволяют сделать важный вывод: ИИ уже стал частью организационной практики, но его внедрение остаётся неравномерным. Крупные компании чаще имеют ресурсы, регламенты, специалистов и инфраструктуру. Малые организации, самозанятые и индивидуальные специалисты могут использовать нейросети ситуативно, без формальных правил проверки качества, источников, конфиденциальности и последствий применения результата.

Это создаёт отдельную группу рисков: не только мошеннических, но и профессиональных. Ошибочный ответ ИИ может попасть в отчёт, коммерческое предложение, юридически значимый текст, публичную публикацию, клиентскую коммуникацию или управленческое решение.

Кризис цифрового доверия: содержание проблемы

Под кризисом цифрового доверия в настоящей работе понимается ситуация, при которой пользователь регулярно сталкивается с цифровыми объектами, требующими оценки достоверности и безопасности, но не обладает достаточными инструментами, знаниями или временем для такой оценки.

К таким объектам относятся:

- сообщения в мессенджерах;
- ссылки;
- документы;
- сайты;
- ответы нейросетей;
- изображения;
- видео;
- голосовые сообщения;
- инвестиционные предложения;
- деловые письма;
- уведомления от якобы официальных организаций;
- тексты, подготовленные ИИ;
- цифровые инструкции и рекомендации.

Кризис цифрового доверия проявляется в двух противоположных формах.

Первая форма — избыточное доверие. Пользователь верит сообщению, ссылке, документу, голосовому обращению или ответу ИИ без проверки. В этом случае повышается риск финансовых потерь, передачи персональных данных, установки вредоносного программного обеспечения, распространения недостоверной информации или принятия ошибочного решения.

Вторая форма — тотальное недоверие. Пользователь не понимает, какие источники надёжны, какие действия безопасны и как отличить достоверное от манипулятивного. Это снижает качество цифрового взаимодействия, повышает тревожность и усложняет использование полезных технологий.

Обе формы вредны. Поэтому задача современной цифровой грамотности заключается не в том, чтобы убедить человека «доверять» или «не доверять», а в том, чтобы сформировать навык проверять до действия.

Классификация пользовательских рисков

На основе анализа статистики и описаний цифровых угроз можно выделить пять групп пользовательских рисков.

1. Информационные риски

К ним относятся:

- использование неподтверждённых ответов ИИ;
- ошибки в фактах, датах, цифрах;
- устаревшая информация;
- искажение смысла источников;
- распространение недостоверных сведений;
- подмена экспертного знания убедительной формулировкой.

Эти риски особенно значимы в профессиональной среде: в аналитике, маркетинге, управлении, образовании, праве, медицине, финансах и публичных коммуникациях.

2. Финансовые риски

К ним относятся:

- переход по фишинговым ссылкам;
- ввод банковских данных на поддельных сайтах;
- перевод денег под давлением;
- инвестиционные предложения с признаками обмана;
- поддельные счета и реквизиты;
- установка вредоносного программного обеспечения;
- передача кодов подтверждения.

Данные Банка России показывают, что социальная инженерия, фишинговые ссылки и вредоносное программное обеспечение остаются актуальными элементами мошеннических схем.

3. Коммуникационные риски

К ним относятся:

- сообщения от имени банка, государственных органов, маркетплейсов, работодателя или родственников;
- просьбы о срочном переводе денег;
- психологическое давление;
- требование сохранить разговор в тайне;
- манипуляции страхом, выгодой или авторитетом;
- поддельные уведомления о выплатах, блокировках, штрафах или проверках.

Особенность этих рисков в том, что они воздействуют не только на техническую систему, но и на психику человека. Мошенническая коммуникация часто строится на срочности, страхе, авторитете, дефиците времени и снижении способности к критической оценке.

4. Документные риски

К ним относятся:

- поддельные договоры;
- поддельные счета;
- несоответствие реквизитов;
- опасные условия предоплаты;
- обещание гарантированной доходности;
- документы от неизвестных контрагентов;
- несоответствие между заявленным отправителем и фактическими данными;
- юридически значимые формулировки, которые пользователь не распознаёт как рискованные.

Эта группа рисков особенно значима для предпринимателей, самозанятых, малого бизнеса и специалистов, которые не имеют постоянного юридического или информационно-безопасностного сопровождения.

5. Профессиональные риски использования ИИ

К ним относятся:

- включение неподтверждённых данных в отчёты;
- подготовка некорректных документов;
- публикация недостоверной аналитики;
- использование ИИ-текстов без проверки источников;
- передача конфиденциальной информации в нейросетевые сервисы;
- зависимость от ИИ без понимания границ его применимости.

Эта группа рисков будет усиливаться по мере распространения ИИ в рабочих процессах.

Почему аудитория 25+ находится в зоне особого риска

Аудитория старше 25 лет представляет особый исследовательский интерес по нескольким причинам.

Во-первых, это экономически активная группа. Люди в этом возрасте чаще принимают финансовые, трудовые, предпринимательские, семейные и управленческие решения.

Во-вторых, эта аудитория активно использует цифровые сервисы: онлайн-банкинг, мессенджеры, маркетплейсы, государственные услуги, дистанционную работу, документы, онлайн-образование и ИИ-инструменты.

В-третьих, цена ошибки для этой группы выше. Ошибочный переход по ссылке, доверие к мошенническому сообщению, использование неподтверждённого ИИ-ответа или подписание рискованного документа может привести к денежным потерям, утечке данных, юридическим последствиям, репутационному ущербу или ошибочному профессиональному решению.

В-четвёртых, часть людей 25–55 лет фактически становится цифровыми посредниками для старших родственников. Пожилые пользователи не всегда готовы самостоятельно проверять сообщения, ссылки или документы, поэтому ответственность за цифровую безопасность семьи часто переходит к более молодым взрослым.

Таким образом, аудитория 25+ является не только пользователем цифровой среды, но и субъектом ответственности: за себя, семью, работу, бизнес, клиентов и финансовые решения.

Необходимость механизмов проверки информации и цифрового риска

Проведённый анализ показывает, что современная цифровая грамотность не может ограничиваться умением пользоваться сервисами. В условиях генеративного ИИ и цифрового мошенничества она должна включать как минимум четыре компонента.

Первый компонент — проверка достоверности информации.
Пользователь должен понимать, какие утверждения требуют источников, какие данные могут быть устаревшими, где ИИ мог сформулировать неподтверждённый вывод.

Второй компонент — проверка источника и контекста.
Недостаточно оценить только текст сообщения. Важно понимать, кто отправитель, куда ведёт ссылка, совпадают ли реквизиты, почему от пользователя требуют срочного действия.

Третий компонент — проверка риска действия.
Ключевой вопрос не только в том, правдива ли информация. Важно понимать, что произойдёт, если пользователь выполнит действие: перейдёт по ссылке, введёт код, подпишет документ, отправит данные, переведёт деньги.

Четвёртый компонент — формирование безопасной поведенческой привычки. Пользователь должен привыкнуть к принципу: сначала проверка, потом действие.

В этом смысле профилактика цифрового мошенничества и ошибок ИИ должна быть не только технической, но и поведенческой. Даже развитая антифрод-система не может полностью устранить риск, если пользователь самостоятельно совершает действие под влиянием давления, доверия, срочности или ошибочного ощущения компетентности.

Полученные выводы позволяют сформулировать несколько положений.

Во-первых, цифровой риск в 2026 году нельзя рассматривать только через призму количества зарегистрированных преступлений. Снижение ИКТ-преступности по данным МВД России является положительной тенденцией, но не отменяет пользовательской уязвимости. На уровне поведения сохраняются сценарии, в которых человек сам совершает рискованное действие под влиянием обмана, давления или доверия.

Во-вторых, генеративный ИИ усиливает не только продуктивность, но и неопределённость. Пользователь получает возможность быстро создавать и получать тексты, изображения, рекомендации и аналитические материалы, но не всегда способен оценить их достоверность. Это особенно важно в ситуациях, связанных с правом, финансами, медициной, безопасностью, бизнесом и публичной коммуникацией.

В-третьих, традиционная цифровая грамотность требует расширения. Раньше она во многом сводилась к навыкам пользования цифровыми сервисами. В новых условиях она должна включать навыки проверки информации, оценки источников, распознавания манипулятивных сценариев, анализа цифрового риска и понимания последствий действия.

В-четвёртых, механизмы проверки должны быть ориентированы не только на объект, но и на действие. Проверка ссылки, сообщения, документа или ответа ИИ имеет практический смысл тогда, когда помогает пользователю принять более безопасное решение.

Ограничения исследования

Настоящая работа имеет ряд ограничений.

Во-первых, официальная российская статистика за полный 2026 год на дату подготовки рукописи отсутствует. Поэтому данные 2026 года представлены только по январю–февралю МВД России.

Во-вторых, статистика МВД России и Банка России отражает разные явления и не может напрямую сопоставляться как единая временная серия. МВД фиксирует преступления в уголовно-правовом контексте, а Банк России — операции без добровольного согласия клиентов финансовых организаций.

В-третьих, официальная статистика пока не всегда выделяет случаи, непосредственно связанные с генеративным ИИ. Поэтому нельзя утверждать, что весь рост цифрового мошенничества вызван искусственным интеллектом. Корректная формулировка состоит в том, что генеративный ИИ является фактором, который может усиливать масштабируемость, убедительность и персонализацию цифровых мошеннических сценариев.

В-четвёртых, работа не включает собственное эмпирическое исследование пользователей. Для дальнейшей проверки выводов необходимы опросы, интервью, фокус-группы и тестирование пользовательских сценариев.

Заключение

В 2023–2026 годах Россия столкнулась с устойчивой трансформацией цифровых рисков. В 2023 году каждое третье преступление было совершено с использованием информационно-телекоммуникационных технологий, а в 2024 году их доля достигла 40%. В 2025 году и начале 2026 года официальная статистика МВД зафиксировала снижение таких преступлений, что свидетельствует об усилении противодействия и профилактики.

Однако данные Банка России показывают, что финансовые мошеннические операции и социальная инженерия сохраняют высокую значимость. В 2025 году объём операций без добровольного согласия клиентов продолжил расти, а количество таких операций увеличилось на 31,2%. Это означает, что цифровой риск не исчезает, а трансформируется: техническая защита усиливается, но пользователь остаётся ключевой точкой воздействия.

Параллельно нейросети стали массовым инструментом. Они используются для поиска информации, советов, текстов, анализа, перевода, изображений, деловой переписки и рабочих задач. Это создаёт новую проблему: пользователь получает быстрый инструмент производства информации, но не всегда обладает навыками проверки её достоверности, источников и последствий применения.

Главный вывод исследования состоит в следующем: цифровая безопасность в эпоху генеративного ИИ должна рассматриваться не только как техническая защита от вредоносных сайтов и программ, но и как система оценки цифрового доверия. Такая система должна помогать человеку оценивать не только объект — ссылку, документ, сообщение или ответ ИИ, — но и риск действия, которое предлагается совершить.

Перспективным направлением становится развитие механизмов проверки информации, цифровых сообщений, документов и ИИ-ответов, а также формирование новой модели цифровой грамотности, основанной на принципе: проверить до действия.

Этическое заявление

Автор заявляет, что несёт полную ответственность за содержание настоящей рукописи. Исследование выполнено на основе открытых статистических и аналитических источников и не включает сбор, обработку или публикацию персональных данных участников. Эксперименты с участием людей или животных не проводились. Информированное согласие участников исследования не требовалось, поскольку эмпирический материал представлен вторичными открытыми данными. Конфликт интересов отсутствует.

Заявление об использовании инструментов искусственного интеллекта

При подготовке рукописи могли использоваться цифровые инструменты на основе искусственного интеллекта для структурирования материала, языковой редактуры и систематизации источников. Ответственность за достоверность данных, корректность ссылок, интерпретацию статистики и итоговые научные выводы несёт автор.