Смирнова Василиса Николаевна, студентка
ОГАПОУ "Ульяновский Авиационный колледж – МЦК"

ТЕХНОЛОГИИ И ОБЩЕСТВО: РАЗРЫВ В ВОСПРИЯТИИ БУДУЩЕГО ГЛАЗАМИ ПРОФЕССИОНАЛОВ И ПОЛЬЗОВАТЕЛЕЙ

Аннотация. Статья исследует различия во взглядах специалистов и пользователей на технологии. На основе анализа трёх исследований выявлен разрыв в оценке рисков и ответственности в сферах облачных вычислений, ИИ и робототехники. Предложены пути повышения цифровой грамотности и формирования осознанного взаимодействия с технологиями

Ключевые слова: Технологии, общество, восприятие, разрыв, профессионалы, пользователи

Современные технологии – облачные системы, искусственный интеллект, робототехника – всё глубже проникают в повседневную жизнь. Однако между теми, кто создаёт эти технологии (специалисты), и теми, кто их использует (пользователи), существует заметный разрыв в восприятии рисков, возможностей и ответственности. На основе данных трёх исследований мы сравниваем взгляды этих двух групп на ключевые технологические тренды и предлагаем пути к более осознанному взаимодействию.

Исследование среди 500 активных пользователей облачных сервисов показало:

Факты использования: 99% респондентов ежедневно используют облачные решения (Google Диск, iCloud, Яндекс.Диск).

Безопасность на практике: только 32% применяют двухфакторную аутентификацию, 15% – менеджеры паролей.

Восприятие ответственности: 87% пользователей считают, что провайдер полностью отвечает за безопасность их данных.

Контраст с позицией специалистов:

Профессионалы в области кибербезопасности подчёркивают модель разделённой ответственности, где пользователь отвечает за настройки, управление доступом и шифрование данных. Яркий пример – утечка данных Capital One (2019) из-за ошибки в настройках брандмауэра AWS.

Опрос пользователей и специалистов в области ИИ выявил:

Пользователи ценят удобство и персонализацию (голосовые помощники, рекомендательные системы), но слабо представляют, как работают алгоритмы.

Специалисты акцентируют внимание на этических рисках: смещение в данных, «чёрный ящик» моделей, проблемы конфиденциальности.

Пример из исследования:

Пользователи охотно используют ИИ-тренеры и симуляторы, но редко задумываются о том, какие данные собираются и как используются.

Разрыв: Пользователи видят поверхностный слой – удобство; специалисты – глубинные риски и системные ограничения.

Исследование среди 200 респондентов (пользователи технологий и инженеры) показало:

Общее видение: 87% пользователей и 92% специалистов считают ИИ и машинное зрение ключевыми технологиями будущего.

Разное восприятие готовности:

Пользователи ожидают быстрого внедрения роботов в быт и сервисы.

Специалисты указывают на технические, регуляторные и этические барьеры.

Оценка рисков:

Пользователи опасаются потери рабочих мест.

Специалисты – киберугроз, сбоев в управлении, проблем безопасности.

Взгляды пользователей и специалистов расходятся по нескольким ключевым аспектам. Пользователи в основном фокусируются на удобстве, доступности и конечном результате использования технологий. Они склонны перекладывать ответственность за безопасность на провайдеров или разработчиков, оценивают риски чаще эмоционально, через призму личного опыта, и ожидают быстрых, практически мгновенных результатов от внедрения новых технологий.

Специалисты же подходят к технологиям системно: их внимание сосредоточено на вопросах безопасности, архитектурных решениях и долгосрочных рисках. Они разделяют ответственность между разработчиком, провайдером и конечным пользователем, оценивают риски на основе данных и глубокого анализа, а также отдают себе отчёт в сложности и постепенности реального внедрения инноваций, понимая, что между идеей и её массовой реализацией лежит длинный путь технических, регуляторных и организационных преодолений.

Рекомендации по сокращению разрыва в восприятии технологий

Для преодоления выявленного разрыва в восприятии технологий между специалистами и пользователями необходимы скоординированные действия всех участников цифровой экосистемы.

Для специалистов и компаний-разработчиков ключевой задачей является создание технологий, ориентированных на человека. Это включает разработку интерфейсов и продуктов с принципом встроенной безопасности (security by design), что минимизирует ошибки конечного пользователя. Не менее важно внедрять прозрачные и понятные механизмы информирования о сборе и использовании данных, а также о потенциальных рисках. Создание доступного образовательного контента – гидов, видеороликов и интерактивных симуляторов – позволит пользователям глубже понять принципы работы используемых ими систем [1, 2].

Со стороны пользователей требуется переход от пассивного потребления к осознанному взаимодействию с технологиями. Это предполагает проявление интереса к базовым настройкам безопасности и политикам конфиденциальности сервисов. Критически важно внедрять рекомендуемые практики защиты, такие как многофакторная аутентификация (MFA), использование менеджеров паролей и регулярное обновление программного обеспечения. Активное участие в опросах, обсуждениях и формирование обратной связи для разработчиков помогает сделать продукты более удобными и безопасными [4].

Регуляторам и общественным институтам отводится роль создания рамок для безопасного и этичного развития цифровой среды. Их усилия должны быть направлены на поддержку и внедрение национальных стандартов цифровой грамотности. Необходимо стимулировать открытый диалог и партнёрство между технологическими компаниями, экспертным сообществом и обществом. Разработка и продвижение этических кодексов, особенно в таких чувствительных областях, как искусственный интеллект и робототехника, станут основой для ответственного внедрения инноваций [2, 3, 5].

Таким образом, сокращение разрыва возможно только через совместные усилия, где каждая сторона принимает на себя часть ответственности за формирование безопасного, понятного и доверительного технологического будущего.

Технологии перестали быть уделом только специалистов – они стали частью повседневной реальности для миллионов. Однако разрыв в восприятии между теми, кто создаёт технологии, и теми, кто их использует, остаётся серьёзным вызовом. Его преодоление требует не только технических решений, но и культурных изменений: повышения цифровой грамотности, развития открытой коммуникации и формирования отношений взаимной ответственности. Только так можно построить цифровое общество, в котором технологии служат людям – безопасно, осознанно и этично

Список литературы:

1. Гартнер. Аналитический прогрос: публичные облачные сервисы в мире: перспективы развития и внедрения. – М.: Издательский дом «Гартнер», 2023. – 45 с.

2. Альянс безопасности облачных вычислений. Основные угрозы облачным вычислениям: ежегодный доклад о трендах и уязвимостях. – М.: Издательство CSA, 2023. – 68 с.

3. Национальный институт стандартов и технологий США. Безопасность и конфиденциальность в облачных вычислениях: практическое руководство для организаций. – Вашингтон: Издательство NIST, 2020. – 120 с.

4. Исследование осведомлённости пользователей облачных сервисов: итоги опроса 500 респондентов о практике использования и понимания безопасности. – Ульяновск: Издательство УАК-МЦК, 2024. – 38 с.

5. Сравнительный анализ восприятия технологий ИИ и робототехники: результаты анкетирования специалистов и конечных пользователей. – Ульяновск: Издательство УАК-МЦК, 2025. – 52 с.

6. Институт SANS. Мониторинг безопасности облаков: комплексные методики и инструменты для непрерывного контроля. – Бетесда: Издательство SANS, 2023. – 85 с