

ЦИФРОВАЯ ОТВЕТСТВЕННОСТЬ КАК ФАКТОР УСТОЙЧИВОГО РАЗВИТИЯ БИЗНЕСА

Шишков Сергей Сергеевич

*студент 1 курса магистратуры Самарского университета,
Россия, г. Самара*

Заводчикова Тамара Борисовна

*к.э.н., доцент кафедры общего и стратегического
менеджмента Самарского университета, Россия, г. Самара*

DIGITAL RESPONSIBILITY AS A FACTOR OF SUSTAINABLE BUSINESS DEVELOPMENT

Shishkov Sergey Sergeevich

*First-year master's student at Samara University,
Russia, Samara*

Zavodchikova Tamara Borisovna

*Candidate of Economic Sciences, Associate Professor of the
Department of General and Strategic Management, Samara University,
Russia, Samara*

АННОТАЦИЯ

В статье рассмотрено влияние цифровых технологий на деятельность современных компаний, исследованы фактические данные по затратам на инновационные технологии, безопасности облачных сервисов, позволившие сделать вывод о возрастающей роли цифровой ответственности в развитии отечественного бизнеса.

ABSTRACT

The article examines the impact of digital technologies on the activities of modern companies, examines the actual data on the costs of innovative technologies and the security of cloud services, which allowed

us to conclude about the increasing role of digital responsibility in the development of domestic business.

Ключевые слова: цифровая ответственность; устойчивое развитие; этика искусственного интеллекта; доверие; цифровая грамотность; цифровая безопасность.

Keywords: digital responsibility; artificial intelligence ethics; trust; digital literacy; cybersecurity; competitive advantage; personal data.

На сегодняшний день цифровые технологии проникают во все сферы бизнеса, меняя способы работы компаний с клиентами, сотрудниками и обществом в целом. Быстрое развитие искусственного интеллекта, анализ больших данных, автоматизация процессов открывают перед организациями новые возможности для устойчивого развития. Однако только инноваций недостаточно. Для долгосрочной конкурентоспособности компании должны внедрять нормы цифровой ответственности, поскольку клиенты всё чувствительнее относятся к тому, как компании ведут цифровой бизнес, и выбирают тех, кто уделяет особое внимание последствиям своих технологических решений.

Компании, игнорирующие этические аспекты цифровой деятельности, сталкиваются с потерей доверия клиентов, уходом сотрудников, штрафами и ухудшением репутации. В то же время организации, делающие акцент на ответственное использование технологий, строят прочные отношения с клиентами, привлекают лучших специалистов и получают преимущество на рынке, создавая основу для долгосрочного развития.

Среди широкого многообразия технологий цифровые данные, искусственный интеллект и Интернет вещей вызывают наибольшие

этические вопросы и активные дискуссии, одновременно представляя большую значимость для успешной цифровой трансформации бизнеса. Эта двойственная роль — источник рисков и драйвер развития — отражена в рыночной динамике: по данным TAdviser, объём рынка кибербезопасности и сопутствующих инновационных технологий с 2021 по 2025 год демонстрирует рост более чем в два раза, что свидетельствует об усиливающемся внимании бизнеса к ответственному управлению этими технологиями (рисунок 1) [2, 4, 5].

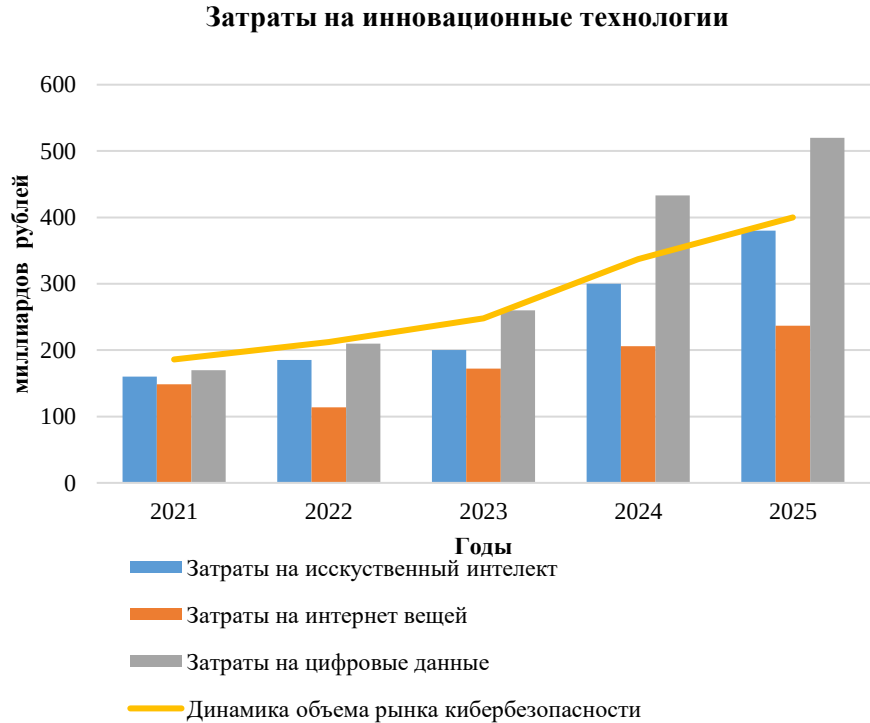


Рисунок 1 - Затраты на инновационные технологии

Представленная динамика затрат демонстрирует рост инвестиций в инновационные технологии. Рост затрат на искусственный интеллект и цифровые данные говорит о стремлении бизнеса повысить эффективность за счет автоматизации процессов. А рост рынка кибербезопасности объясняется важностью безопасного хранения персональных данных пользователя для компании [6].

Исходя из динамики роста рынка инновационных технологий, особую значимость приобретает цифровая ответственность. Она подразумевает использование инноваций наиболее прозрачно, справедливо и безопасно. При этом цифровая ответственность обуславливается совокупностью внутренних факторов, действующих на разных уровнях [7].

В первую очередь стоит выделить рыночные и репутационные факторы, которые основываются на доверии. Они напрямую связаны со стремительным ростом использования облачных сервисов для хранения данных о пользователе и увлечением объема утечек персональных данных (рисунок 2) [8].

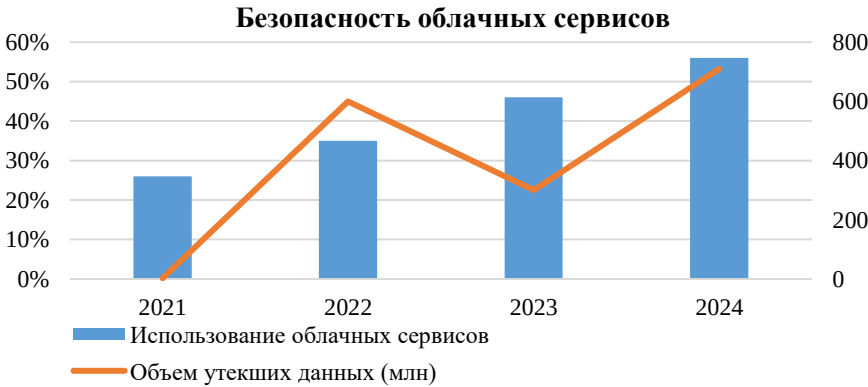


Рисунок 2- Безопасность облачных сервисов

Исходя из данных, представленных аналитической платформой TAdviser, использование облачных сервисов показывает стабильный рост из года в год. Что говорит о том, что все большее количество информации концентрируется в цифровых средах. А согласно статистике представленной Роскомнадзором, количество утечек в 2024 году значительно увеличилось по сравнению с 2021 годом. Несмотря на рост затрат на кибербезопасность (рисунок 1), облачные данные остаются уязвимыми, кибератаки становятся все чаще и масштабнее, затрагивая облачные данные крупных компаний [7].

Современный пользователь интернета хорошо понимает, какие угрозы могут возникнуть при передаче личной информации — будь то телефонный номер или данные паспорта. Он ожидает, чтобы компания, получившая эти сведения, надёжно, добросовестно и внимательно относилась к обработке своих персональных данных.

Следующий фактор — социальный, он подразумевает то, как пользователи воспринимают инновационные технологии. На основе статистики представленной аналитическим центром НАФИ и акцией «Цифровой Диктант», рассмотрим индекс цифровой грамотности в период с 2020 по 2024 годы (рисунок 3) [1, 3]. При помощи данного индекса, можно определить восприятие пользователями инновации за выделенный период.

Статистика выявляет снижение показателей цифрового потребления и цифровых компетенций, однако динамика цифровой безопасности в период 2023-2024 года демонстрирует рост, достигнув максимума в 7,2 балла. Рост динамики цифровой безопасности обусловлен увеличением утечек персональных данных (рисунок 2). Пользователи все более избирательнее

относятся к выбору компаний и беспокоятся за сохранность своих данных [3].

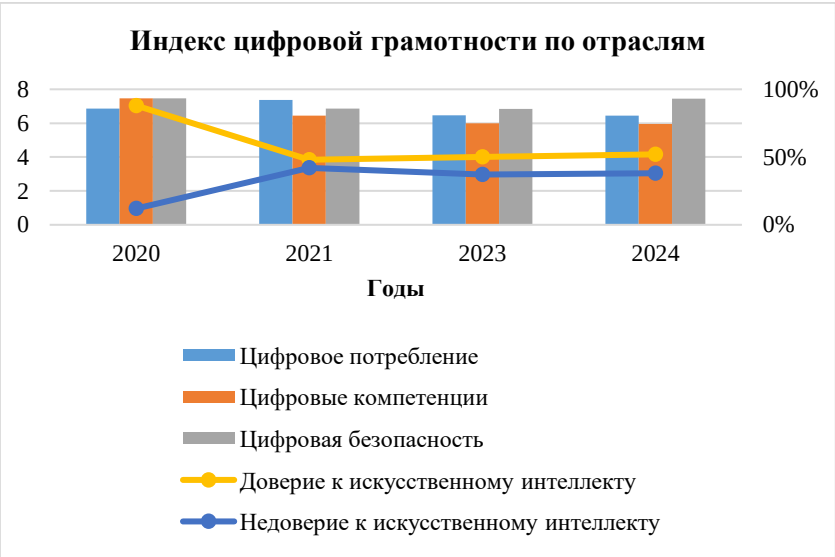


Рисунок 3- Индекс цифровой грамотности по отраслям

Стоит сказать о том, что на фоне роста затрат на инновации (рисунок 1), процент недоверия пользователей к искусственному интеллекту растет, в то время как процент пользователей, доверяющих искусственному интеллекту, уменьшается. Возможно, это связано со стремительным развитием самих инноваций и пользователи не всегда успевают адаптироваться к ним.

Результат проведенного исследования позволил выявить динамику затрат на инновационные технологии и безопасность облачных сервисов. Анализ показал, что факторы цифровой ответственности напрямую влияют на то, как компанию воспринимают пользователи. Важно понимать, какие факторы

наиболее значимы для конкретной организации с учетом специфики ее деятельности. При этом создание прозрачной и безопасной цифровой среды является основой для обеспечения устойчивого развития бизнеса.

Список литературы:

1. Доверие к ИИ: мониторинг общественного мнения [Электронный ресурс] / ВЦИОМ. – 2024. – URL: <https://wciom.com/press-release/trust-in-ai> (дата обращения: 12.02.2026).
2. Доклад о развитии электронной торговли, 2024: Обзор [Электронный ресурс] / UNCTAD. – Женева, 2024. – URL: https://unctad.org/system/files/official-document/der2024_overview_ru.pdf (дата обращения: 12.02.2026).
3. Индекс цифровой грамотности 2024: цифровая грамотность россиян не растёт третий год подряд [Электронный ресурс] / Аналитический центр НАФИ. – 2025. – URL: <https://nafi.ru/analytics/indeks-tsifrovoy-gramotnosti-2024-tsifrovaya-gramotnost-rossiyan-ne-rastet-tretyy-god-podryad/> (дата обращения: 12.02.2026).
4. Интернет вещей, IoT (рынок России) [Электронный ресурс] // TAdviser. – URL: <https://surl.li/xqianl> (дата обращения: 12.02.2026).
5. ИТ-рынок России [Электронный ресурс] // TAdviser. – URL: <https://inlnk.ru/20V7Qo> (дата обращения: 12.02.2026).
6. Национальная стратегия развития искусственного интеллекта до 2030 года [Электронный ресурс]. – URL: <https://inlnk.ru/70A3RG> (дата обращения: 12.02.2026).

7. Расходы на цифровую трансформацию [Электронный ресурс] // TAdviser. – URL: <https://inlnk.ru/yO59Ky> (дата обращения: 12.02.2026).

8. Роскомнадзор зафиксировал 135 утечек баз данных в 2024 году [Электронный ресурс] // Forbes. – 2024. – URL: <https://inlnk.ru/G6J3Qj> (дата обращения: 12.02.2026).

References:

1. Trust in AI: monitoring public opinion [Electronic resource] / VTsIOM. – 2024. – URL: <https://wciom.com/press-release/trust-in-ai> (date of access: 02/12/2026).

2. Report on the development of electronic commerce, 2024: Review [Electronic resource] / UNCTAD. – Geneva, 2024. – URL: https://unctad.org/system/files/official-document/der2024_overview_ru.pdf (date of request: 12.02.2026).

3. Digital Literacy Index 2024: the digital literacy of Russians has not grown for the third year in a row [Electronic resource] / NAFI Analytical Center. – 2025. – URL: <https://nafi.ru/analytics/indeks-tsifrovoy-gramotnosti-2024-tsifrovaya-gramotnost-rossiyan-ne-rastet-tretiy-god-podryad-> / (date of access: 02/12/2026).

4. Internet of Things, IoT (Russian market) [Electronic resource] // TAdviser. – URL: <https://surl.li/xqianl> (date of access: 02/12/2026).

5. IT market of Russia [Electronic resource] // TAdviser. – URL: <https://inlnk.ru/20V7Qo> (date of request: 12.02.2026).

6. National strategy for the development of artificial intelligence until 2030 [Electronic resource]. – URL: <https://inlnk.ru/70A3RG> (date of access: 12.02.2026).

7. Expenses for digital transformation [Electronic resource] // TAdviser. – URL: <https://inlnk.ru/yO59Ky> (date of access: 02/12/2026).

8. Roskomnadzor recorded 135 database leaks in 2024 [Electronic resource] // Forbes. – 2024. – URL: <https://inlnk.ru/G6J3Qj> (date of request: 12.02.2026).