Кыялбекова Элина Кыялбековна
студентка
Научный руководитель
Губанова Анна Викторовна
преподаватель
Красноярский филиал ФГОБУ ВО «Финансовый университет
при Правительстве Российской Федерации»
г. Красноярск, Красноярский край

«ТЕМНАЯ СТОРОНА» ДАННЫХ НОВЫЕ РИСКИ И ВЗГЛЯД ПОКОЛЕНИЯ Z В КРАСНОЯРСКЕ

Аннотация: *статья посвящена исследованию «тёмной стороны» цифровой трансформации, рассматриваются такие риски, как киберугрозы, смещения алгоритмов и цифровая зависимость. На основе опроса студентов выявлен критический разрыв между сложностью технологических угроз и цифровой наивностью поколения Z, что создаёт для бизнеса серьёзные репутационные и этические риски. Делается вывод о необходимости интеграции управления цифровыми рисками в корпоративную стратегию, включая развитие прозрачности и алгоритмической грамотности. Утверждается, что ответственное управление данными и ИИ становится новым источником конкурентного преимущества и доверия в цифровой экономике.*

Ключевые слова: *цифровая трансформация, корпоративные риски, поколение Z, алгоритмическая грамотность, кибербезопасность, ответственный ИИ.*

Цифровая трансформация, долгое время воспринимавшаяся как безусловный источник эффективности и конкурентных преимуществ, открыла новую, «тёмную сторону». Данные, ставшие «новой нефтью», порождают комплекс рисков, способных подорвать устойчивость бизнеса, репутацию и финансовые результаты. Советам директоров и топ-менеджменту сегодня необходимо управлять не только традиционными бизнес-процессами, но и тремя критическими

угрозами цифровой эпохи, такими как киберугрозы, скрытыми смещениями алгоритмов и формирующейся цифровой зависимостью.

С одной стороны, внедрение искусственного интеллекта (ИИ) кардинально ускорило время принятия решений и глубину анализа [1]. С другой стороны, эта же зависимость от данных сделала корпорации крайне уязвимыми. Киберпреступность превратилась в высокодоходную индустрию, где атаки нацелены не только на кражу финансов, но и на шпионаж, саботаж и получение контроля над инфраструктурой. По данным исследований, средняя стоимость утечки данных в 2023 году достигла исторического максимума, что напрямую ударило по прибыли и капитализации компаний [2].

С каждым годом проблема утечки данных становится более актуальной, так, например, в 2025 году, хакерская группировка «BO Team» атаковали инфраструктуру провайдера «Орион Телеком», похитив данные пользователей. Этот инцидент подчеркивает уязвимость даже крупных компаний и важность защиты личной информации клиентов. В условиях таких угроз особенно важно понимать, как молодое поколение осознает риски, связанные с цифровыми технологиями. Поэтому мы провели опрос среди студентов Красноярских вузов и СПО (СФУ, КГПУ, СибГУ, Красфин, КМК), чтобы выяснить, как цифровое поколение воспринимает новые корпоративные риски и насколько они готовы к вызовам, которые ставит современный киберпространство.

Исследование цифровой осознанности студентов Красноярска.

Вопрос 1. Какая угроза кажется вам наиболее реальной для компаний Красноярска?

1. Утечка персональных данных (45%).

2. Сбой в алгоритмах банков (35%).

3. Хакерская атака на городские сервисы (20%).

Наши выводы: Студенты проявляют высокую чувствительность к приватности, но воспринимают кибератаки как локальные инциденты с данными, а не как

системную угрозу бизнесу. Вероятно, студенты чаще сталкивались с алгоритмическими ошибками в банковских приложениях, чем с масштабными хакерскими атаками, это показывает их картину рисков.

Вопрос 2. Кому вы больше доверяете в принятии важных решений?

Ответы студентов:

1) алгоритму (55);

2) человеку (30%);

3) затрудняюсь ответить (15%).

Наши выводы: Поколение Z демонстрирует «цифровую наивность» – веру в объективность алгоритмов. Это создает серьезный риск: внедряя AI-системы в HR, кредитование, будущие сотрудники и клиенты не будут подвергать их решения критической проверке. В Красноярске, где IT-кластер активно развивается, это особенно важно для компаний, внедряющих скоринг и автоматизацию.

Вопрос 3. Что для вас значат персональные данные?

Ответы студентов.

1. Это валюта, которую я готов обменять на удобство (50%).

2. Это приватность, которую нужно защищать (40%).

3. Не задумываюсь об этом (10%).

Наши выводы: половина инвестирует свои данные в комфорт, получая «здесь и сейчас» удобные сервисы и бонусы. Другая половина копит эту ценность, предпочитая сохранить ее в тайне, чтобы почувствовать себя защищенным. Таким образом, вопрос уже не в том, замечают ли люди ценность данных, а в том, что они предпочитают с ними делать: тратить или сохранить.

Вопрос 4. Что вы почувствовали, когда на сутки отключили все онлайн-сервисы в городе?

Ответы студентов.

1. Панику и дискомфорт (40%).

2. Облегчение и отдых от цифры (35%).

3. Не заметил разницы (25%).

Наши выводы: реакция раскрывает глубину цифровой зависимости. Мы живем в эпоху, когда почти половина из нас спокойно меняет личную информацию на скидки и удобные приложения, а вторая половина постоянно начеку и старается защитить свои данные. При этом нам кажется, что мы контролируем ситуацию, хотя на самом деле мы просто привыкли к этому новому порядку вещей и уже не представляем жизни без интернета, даже те, кто переживает за приватность.

Вопрос 5. Кто должен нести ответственность за утечку данных?

Ответы студентов.

1. Компания, которая не защитила данные (60%).

2. Государство через законы и контроль (25).

3. Сам пользователь (15%).

Наши выводы: четкое ожидание корпоративной ответственности. После инцидентов с утечками данных в красноярских компаниях в 2023 году, студенты сформировали запрос на прозрачность и безопасность. Это прямое указание бизнесу: инвестиции в кибербезопасность и прозрачная политика данных станут конкурентным преимуществом при работе с молодежью.

Ключевые выводы.

1. Студенты осознают ценность данных, но часто принимают их сбор как неизбежность. Это создает риск «согласия по умолчанию», когда пользователи автоматически принимают условия, не оценивая рисков.

2. Доверие к алгоритмам превышает доверие к людям.

3. Региональная специфика, так как в условиях Красноярска с его климатом и географией цифровая зависимость имеет особое измерение. Сбои воспринимаются острее, но и ценность «живого» взаимодействия сохраняется.

4. Опыт локальных инцидентов с утечкой данных сформировал запрос на корпоративную ответственность. Репутационные риски от утечек для бизнеса в Красноярске особенно высоки при работе с молодежной аудиторией.

Рекомендации для бизнеса Красноярского края.

1. Образовательные инициативы по цифровой грамотности – не как лекции о безопасности, а как диалог о ценности данных и алгоритмической грамотности.

2. Прозрачность как стратегия – открытые политики использования данных, простые соглашения, отчеты об инцидентах повысят доверие молодых клиентов.

3. Тестирование AI-решений на «цифровую наивность» – при внедрении алгоритмов учитывать, что молодые пользователи могут не заметить ошибок.

4. Создание гибридных сервисов – учитывая амбивалентность (зависимость + желание детокса), предлагать варианты как цифрового, так и человеческого взаимодействия.

Исследование среди студентов Красноярска выявило критический риск для корпоративного управления: разрыв между цифровой наивностью пользователей и сложностью технологических угроз.

Поколение Z:

– доверяет алгоритмам больше, чем людям (55%);

– готово обменивать данные на удобство (50%);

– возлагает ответственность за безопасность на компании (60%).

Это создает «ловушку доверия»: бизнесы, внедряющие сложные AI-системы, получают некритично доверяющую аудиторию, что повышает репутационные риски при любом сбое или этическом провале алгоритма.

Управление «тёмной стороной» данных теперь включает управление цифровой культурой потребителей и сотрудников. Недостаточно внедрить этичный AI – нужно формировать алгоритмическую грамотность. Недостаточно защитить данные – нужно объяснять, как и зачем это делается. Компании Красноярского края, которые сделают прозрачность и цифровое образование частью своей бизнес-модели, получат не только защиту от рисков, но и лояльность нового поколения, для которого данные – уже не «нефть», а часть социального договора с бизнесом.

В то же время внутренние риски зачастую не менее опасны, чем внешние. Алгоритмы, управляющие кредитным скорингом, наймом персонала, ценообра-

зованием или логистикой, могут содержать неумышленные, но системные смещения. Такие смещения, унаследованные от исторических данных или заложенные разработчиками, ведут к дискриминации клиентов, неэффективным управленческим решениям и, как следствие, к серьёзным репутационным и судебным издержкам [3]. Регуляторы по всему миру, в частности в ЕС с его «Актом об ИИ», уже вводят жёсткие требования к прозрачности и проверке алгоритмических систем, что создаёт новые комплаенс-риски [4].

Опираясь на анализ, для современного корпоративного управления становятся критически важными следующие выводы.

1. Кибербезопасность перестала быть исключительно ИТ-функцией и стала стратегическим вопросом совета директоров, требующим регулярных аудитов, сценарного планирования и выделения бюджета.

2. Активное развитие внутренней экспертизы в области этики ИИ и алгоритмической аудита как необходимого элемента системы внутреннего контроля и управления рисками (ERM).

3. Смещение фокуса при оценке цифровых активов – от простого внедрения к анализу их устойчивости, прозрачности и потенциала формирования скрытых рисков.

4. Усиление роли комитетов по рискам и аудиту в надзоре за цифровой трансформацией, включая утверждение политик использования данных и алгоритмов [5].

Перспективы управления компанией в цифровую эпоху остаются сложными, а риски будут только эволюционировать. К ним добавляются: растущее регулирование цифрового пространства, геополитическая фрагментация интернета и технологий, а также дефицит квалифицированных кадров в области кибербезопасности.

Важно подчеркнуть, что компании, которые смогут интегрировать управление «тёмной стороной» данных в свою корпоративную ДНК – открыто обсуждая риски, внедряя принципы ответственного ИИ и создавая отказоустойчивые архи-

тектуры, – не только снизят угрозы, но и сформируют новое, устойчивое конкурентное преимущество, основанное на доверии. Это сделает их лидерами в новой, гораздо более требовательной цифровой экономике [3].

Список литературы

1. Воронов М.В. Системы искусственного интеллекта : учебник и практикум / М.В. Воронов, В.И. Пименов, И.А. Небаев. – 2026.

2. Валько Д.В. Экономическая безопасность : учебник для вузов / Д.В. Валько. – 2026.

3. Мировая экономика и международные экономические отношения в условиях полицентризма / под ред. О.В. Буториной, Э.Н. Смирнова. – 2024.

4. Аксёнов А.П. Фондовые рынки развивающихся стран: анализ и инвестиционные стратегии / А.П. Аксёнов, М.Д. Лысенко. – 2022.

5. Звонова Е.А. Глобальные финансы: новые реалии и тренды / Е.А. Звонова, А.С. Булатов. – 2023.

6. Красноярский провайдер «Орион телеком» опроверг утечку данных в результате кибератаки.. – URL: https://gornovosti.ru/news/krasnoyarskiy-provayder-orion-telekom-oproverg-utechku-dannykh-v-rezultate-kiberataki/ (дата обращения: 23.02.2026).