

4. НАПРАВЛЕНИЯ МИНИМИЗАЦИИ РИСКОВ В ПРОЦЕССАХ УПРАВЛЕНИЯ ВЗАИМОДЕЙСТВИЕМ С КЛИЕНТАМИ

Шестакова А.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Князькова В.С. – канд. экон. наук

Проведен анализ рисков, возникающих в процессе цифровизации управления взаимодействием с клиентами, а также разработке направлений по их минимизации. Исследование охватывает организационные, технические, финансовые и репутационные угрозы, с которыми сталкиваются компании при внедрении цифровых технологий, и предлагает стратегические и операционные меры по снижению их воздействия. Для подготовки материалов использовались издания в сфере информационных технологий, сайты рейтинговых агентств Gartner и Forrester, издания научной электронной библиотеки Российского фонда фундаментальных исследований, кейс-стади компаний, интервью с экспертами в области информационных технологий и управления клиентскими отношениями.

Управление взаимодействием с клиентами включает в себя организацию и оптимизацию всех процессов, направленных на установление, поддержание и развитие отношений с потребителями продукции или услуг. В условиях цифровой трансформации эти процессы становятся более сложными и подверженными новым типам рисков.

Актуальность темы обусловлена быстрым развитием цифровых технологий, которые влияют на все аспекты взаимодействия с клиентами. Компании, стремящиеся быть конкурентоспособными, вынуждены внедрять инновационные решения для улучшения качества обслуживания и повышения клиентской лояльности. Однако, с этим возникают новые риски, такие как утечка данных, кибератаки и сбои в работе систем. Эти угрозы могут привести к серьезным финансовым и репутационным потерям. Усиление зависимости от цифровых платформ увеличивает уязвимость бизнеса, что требует разработки эффективных мер по минимизации этих рисков. Важно, чтобы стратегии цифровизации сочетались с надежными мерами по защите данных и обеспечению бесперебойной работы систем. Таким образом, тема минимизации рисков в процессе цифровизации становится все более актуальной для обеспечения устойчивости и безопасности бизнеса.

Цифровизация управления клиентским взаимодействием предоставляет компаниям новые возможности — от автоматизации процессов до повышения точности персонализации. Однако с внедрением цифровых решений возрастает и число рисков, способных негативно повлиять на

устойчивость бизнеса и доверие со стороны клиентов. Важно своевременно выявлять эти риски и внедрять стратегии их минимизации для сохранения эффективности и конкурентных преимуществ [1].

Технические риски связаны с перебоями в работе цифровых платформ, зависимостью от программных решений и нестабильностью инфраструктуры. Если цифровые каналы становятся единственным способом взаимодействия с клиентами, их сбой приводит к полной остановке коммуникации. Также риском является отсутствие резервных систем и инструментов экстренного восстановления. Ярким примером можно назвать сбой в системе бронирования авиабилетов Lufthansa в 2023 году, когда клиенты по всему миру не смогли зарегистрироваться на рейсы. Проблема возникла из-за сбоя в дата-центре и затронула тысячи пользователей. В результате компания понесла значительные имиджевые и финансовые потери [2].

Киберугрозы представляют собой один из наиболее чувствительных рисков цифровизации — это утечки данных, взломы и фишинг. Современные платформы обрабатывают большое количество персональных данных клиентов, что делает их привлекательной целью для атак. Потеря или компрометация информации ведёт к штрафам, судебным искам и снижению доверия. Примером служит утечка данных в результате кибератаки на British Airways в 2018 году, в результате которой были похищены данные более 500 тысяч клиентов [3]. Компания получила штраф в размере 183 миллионов фунтов и столкнулась с негативной реакцией клиентов и СМИ. Этот случай стал прецедентом и показал необходимость постоянного обновления систем безопасности.

Организационные риски возникают при недостаточной подготовке персонала к работе с цифровыми инструментами, особенно в условиях быстрого внедрения новых технологий. Без обучения и инструктажа сотрудники могут использовать системы неэффективно или с ошибками. Это снижает качество обслуживания и ведёт к росту клиентских претензий. Например, в одной из телеком-компаний при переходе на новую CRM-систему сотрудники не прошли должное обучение [4]. В результате обращения клиентов обрабатывались медленно, с ошибками и пропусками. Уровень удовлетворённости снизился, и компании пришлось временно вернуться к прежней системе обслуживания.

Финансовые риски связаны с перерасходом бюджета на внедрение цифровых решений, особенно при неправильной оценке масштабов проекта. Часто инвестиции в цифровизацию не окупаются из-за слабой подготовки, отсутствия тестирования или выбора неэффективных подрядчиков. Это может вызвать заморозку других проектов и ухудшение финансового положения компании. Ярким примером является неудачный выход ритейлера Target на канадский рынок, сопровождавшийся масштабным внедрением ИТ-инфраструктуры без должной отладки [5]. Из-за ошибок в системах учёта и логистики компания понесла убытки более чем на \$2 млрд и была вынуждена закрыть все магазины в стране. Этот пример подчёркивает важность финансового планирования и поэтапного внедрения решений.

Репутационные риски проявляются при негативной реакции клиентов на цифровые нововведения, особенно если сервис становится менее удобным или нестабильным. Ошибки в коммуникации, массовые сбои или агрессивный маркетинг через цифровые каналы могут привести к оттоку клиентов. Репутационные потери часто имеют долговременный эффект и отражаются на выручке. Например, один из крупных банков в 2022 году ошибочно разослал клиентам уведомления с неправильными суммами задолженности [6]. Это вызвало шквал жалоб в социальных сетях и в СМИ, несмотря на оперативное исправление ошибки. В результате уровень доверия к цифровым каналам банка снизился, а компания потеряла часть клиентов.

Для эффективной минимизации рисков цифровизации в управлении взаимодействием с клиентами необходим комплексный подход, включающий технические, организационные и стратегические меры. В первую очередь, важно внедрять стратегии цифровой безопасности, включающие многоуровневую защиту данных, шифрование, системы мониторинга угроз и регулярные аудиты ИТ-инфраструктуры. Это позволяет своевременно выявлять уязвимости и предотвращать атаки, обеспечивая устойчивость систем.

Вторым направлением является регулярное обучение сотрудников и повышение их цифровой грамотности. Персонал должен уметь пользоваться современными цифровыми инструментами, понимать базовые принципы кибербезопасности и быстро адаптироваться к новым технологиям. Это снижает вероятность ошибок, возникающих по причине некомпетентности, и повышает общую эффективность клиентского сервиса [7].

Также рекомендуется использовать резервные каналы коммуникации и технической поддержки. При сбоях в основной системе клиент должен иметь возможность быстро связаться с компанией через альтернативные средства, например, телефон, e-mail, социальные сети или отдельные сервисные платформы. Это позволяет избежать полной остановки коммуникации и поддерживать лояльность клиентов даже в кризисных ситуациях.

Поэтапное внедрение цифровых решений с обязательным тестированием на пилотных группах помогает избежать масштабных сбоев и оперативно выявлять слабые места. Такой подход позволяет

*61-я Научная Конференция Аспирантов, Магистрантов и Студентов БГУИР,
Минск 2025*

корректировать ошибки до масштабного запуска и снижает риски, связанные с несовместимостью или техническими сбоями [8]. Это особенно актуально для крупных CRM-систем и платформ с высокой нагрузкой.

Наконец, важно обеспечить прозрачность работы с клиентскими данными и строго соблюдать действующие нормативы и стандарты защиты информации. Открытая политика конфиденциальности, четкое информирование клиентов о том, как используются их данные, а также соответствие требованиям законодательства (например, GDPR) укрепляют доверие и формируют позитивный имидж компании [9].

Таким образом, минимизация рисков требует системной работы на всех уровнях — от технологий и персонала до стратегий и регламентов взаимодействия с клиентами. Только интеграция этих мер позволяет не просто защищаться от угроз, но и использовать цифровизацию как инструмент устойчивого развития и повышения конкурентоспособности.

В заключении отметим, что риски цифровизации в управлении взаимодействием с клиентами являются значимым фактором, способным повлиять на эффективность бизнеса и доверие со стороны клиентов. Технические сбои, киберугрозы, организационные трудности, финансовые издержки и репутационные потери — всё это потенциальные последствия неудачного внедрения цифровых решений. Однако осознанный и системный подход к управлению этими рисками позволяет существенно снизить уязвимость компании.

Список использованных источников:

- 1.Беляцкая Т. Н. Электронно-информационный компонент товара как основа функционирования организации в условиях ее цифровизации // Инструменты стратегического менеджмента и маркетинга. — Ставрополь: Изд-во СКФУ, 2019. — 290 с.
2. Gartner. Top Strategic Technology Trends. — <https://www.gartner.com> (дата обращения: 02.04.2025).
3. Forrester Research. Customer Experience and Digital Transformation Report. — <https://www.forrester.com> (дата обращения: 03.04.2025).
4. Oracle. How AI and Chatbots Reduce Customer Service Costs. — <https://go.oracle.com> (дата обращения: 04.04.2025).
5. Salesforce. State of the Connected Customer Report. — <https://www.salesforce.com> (дата обращения: 05.04.2025).
6. Чумаченко Д. В., Чернышев С. Н. Управление рисками в цифровой экономике // Вестник университета. — 2022. — №8. — С. 65–72.
7. McKinsey & Company. Digital Risk: Managing Technology Transformation. — <https://www.mckinsey.com> (дата обращения: 05.04.2025).
8. Бауман А. Ю. Информационная безопасность в бизнес-процессах цифровой трансформации // Информационные технологии и телекоммуникации. — 2021. — №4. — С. 38–43.
9. Киселева Н. В. Цифровая трансформация и ее влияние на управление взаимодействием с клиентами // Экономика и предпринимательство. — 2023. — №6(139). — С. 112–116.