

## ЦИФРОВИЗАЦИЯ БАНКОВСКИХ ПРОЦЕССОВ И ЕЕ ВЛИЯНИЕ НА РЕАЛИЗАЦИЮ РИСКОВ

**У. Н. Селивончик**

*аспирант, Белорусский государственный университет, г. Минск, Беларусь, ulianas2001@gmail.com*

**Научный руководитель Л. И. Стефанович**

*доктор экономических наук, профессор, Белорусский государственный университет, г. Минск, Беларусь, L.Stefanovich@tut.by*

Статья посвящена анализу влияния цифровизации банковских процессов на реализацию рисков. В статье рассматриваются современные направления цифровизации, используемые банками в рамках совершенствования своей деятельности и оптимизации внутренних процессов, а также подверженность банков рискам, возникающих в таких процессах. В статье также раскрывается роль и необходимость обеспечения кибербезопасности в банковском секторе.

**Ключевые слова:** банк; банковские процессы; банковские риски; кибербезопасность; цифровизация.

## DIGITALIZATION OF BANKING PROCESSES AND ITS IMPACT ON RISK MANAGEMENT

**U. N. Selivonchik**

*PhD student, Belarusian State University, Minsk, Belarus, ulianas2001@gmail.com*

**Supervisor L. I. Stefanovich**

*doctor of economics, professor, Belarusian State University, Minsk, Belarus, L.Stefanovich@tut.by*

The article analyzes the impact of digitalization of banking processes on risk management. It examines modern digitalization trends used by banks to improve their operations and optimize internal processes, as well as their exposure to risks arising from such processes. The article also explores the role and necessity of cybersecurity in the banking sector.

**Keywords:** bank; banking processes; banking risks; cybersecurity; digitalization.

В условиях стремительного развития финансовых технологий и цифровой трансформации банковских процессов особую актуальность приобретает проблема изменения структуры и характера банковских рисков. Цифровизация затрагивает практически все процессы в банках – от дистанционного обслуживания клиентов до автоматизации внутренних операций и внедрения систем искусственного интеллекта. С одной стороны, это повышает эффективность, снижает транзакционные издержки и расширяет доступ к финансовым услугам. С другой стороны, цифровая трансформация формирует новые источники угроз, включая киберриски, риски алгоритмических ошибок, а также зависимость от внешних технологических провайдеров.

Базельским комитетом по банковскому надзору в 2024 г. был опубликован доклад «Digitalisation of finance», определяющий основные направления цифровизации в финансовой сфере, в том числе банковских процессов.

Комитетом были выделены следующие направления цифровизации:

- интерфейсы прикладного программирования (API) (способствуют оптимизации обмена данными между двумя приложениями и обеспечению проведения банковских операций посредством передачи данных между внутренними системами банка и системой банка и другими организациями (например, в случае передачи функции банка на аутсорсинг);

- искусственный интеллект и машинное обучение (повышают операционную эффективность банка в области обработки данных, предоставляют новые возможности управления рисками, включая такие области применения, как кредитный андеррайтинг, управление нормативным капиталом и ликвидностью, их планирование, выявление и предотвращение легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения (ПОД/ФТ);

- технологии распределительного реестра (позволяют снизить затраты и повысить эффективность проведения транзакций за счет неизменяемого хранения данных, цифровой идентификации и автоматизации процессов);

- облачные вычисления (совместное использование вычислительных ресурсов по требованию, способствующее повышению эффективности и экономии за счет масштаба посредством упрощения доступа к технологиям и вычислительной инфраструктуре) [1].

Наиболее распространенным видом цифровизации банковских процессов является использование машинного обучения. В отличие от традиционных статистических методов, основанных на фиксированных моделях, алгоритмы машинного обучения способны:

- автоматически адаптироваться к изменению данных и выявлять нелинейные зависимости;

- анализировать большие объемы разнородных данных (например, транзакционные данные, кредитные истории, макроэкономические показатели);

- повышать точность прогнозов за счет использования сложных моделей [2].

Кроме того, оптимизация процессов обработки данных, в частности больших данных, является одним из приоритетных направлений в области цифровизации банковских процессов. В рамках данной области банки подвергаются методологическому риску. При работе с большими данными банки используют, в том числе, альтернативные (нетрадиционные) данные (данные, которые ранее не использовались банком), в связи с чем должное внимание должно уделяться выбору таких данных, их обработке и агрегации, выбору аналитических инструментов для интеграции анализа таких данных с традиционными в целях предотвращения использования банками искаженной информации или дезинформации.

При построении моделей, основанных на больших данных, банки также подвергаются такому виду методологического риска, как модельный. В докладе «Использование больших данных в финансовом секторе и риски финансовой стабильности» Банк России обращает внимание на проблему черного ящика (black box problem) при использовании искусственного интеллекта при обработке больших данных, заключающуюся в невозможности перепроверить результат обработки данных, заложенных в модель, искусственным интеллектом [3, с. 16]. Неполное понимание функционирования различных форм аналитики больших данных и качества данных или моделей может привести к реализации модельного риска. В то же время реализация методологического и модельного рисков может привести к системной реализации всех рисков банка. Неправильно выбранные данные и их анализ может привести к искажению получаемой информации и подвергнуть банки к получению убытков (потерь).

Классическим примером влияния цифровизации, как процесса внедрения новых технологий, на реализацию банковских рисков является операционный риск, в частности такие его виды, как технический риск, риск в сфере информационных технологий (ИТ-риск), риск в

сфере информационной безопасности, риск операции и риск использования услуг третьей стороны, в частности риск аутсорсинга (терминология используется в соответствии с Инструкцией об организации корпоративном управлении, утвержденной постановлением Национального банка Республики Беларусь от 21 февраля 2024 г. № 62) [4].

Большинство новых технологических решений, внедряемых в банковские процессы, банки не разрабатывают самостоятельно, а приобретают у поставщиков таких технологий исходя из экономической эффективности. В связи с этим банки все больше подвергаются риску использования услуг третьей стороны, в частности риску аутсорсинга. К видам риска аутсорсинга относятся риск контрагента, риск концентрации, риск отсутствия стратегии выхода из договора аутсорсинга и репутационный риск [5]. Реализация риска отсутствия стратегии выхода из договора аутсорсинга, подразумевающего вероятность невозможности осуществления банком функции, переданной на аутсорсинг самостоятельно либо понесения банком крупных затрат на ее возобновление, может стать критической ситуацией для банка и привести к приостановке его деятельности.

Важно отметить, что современный банковский сектор является одной из наиболее уязвимых сфер для киберугроз ввиду высокой концентрации финансовых ресурсов и персональных данных клиентов. В условиях стремительной цифровой трансформации банковских процессов возрастает необходимость комплексного подхода к обеспечению кибербезопасности и управлению рисками, возникающих посредством внешних атак на внутренние процессы банка. Цифровизация играет в этом процессе ключевую роль, обеспечивая новые возможности для защиты информации, противодействия кибератакам и повышения устойчивости банковской инфраструктуры. В таблице представлены основные направления цифровизации в области обеспечения кибербезопасности банков.

#### Направления цифровизации в области обеспечения кибербезопасности банков

Направления цифровизации	Область применения
Комплексные системы защиты	Создание интегрированных платформ кибербезопасности, включающие мониторинг сетевой активности, управление доступом, автоматизированный анализ событий безопасности (SIEM-системы). Благодаря этому обеспечивается централизованное выявление и реагирование на угрозы, что значительно сокращает время нейтрализации инцидентов
Защита клиентских данных	Обеспечение безопасности персональных и финансовых данных клиентов, посредством шифрования, токенизации, а также технологий защищенного облачного хранения
Цифровая идентификация и аутентификация	Снижение вероятности несанкционированного доступа к банковским сервисам за счет внедрения биометрических методов идентификации и многофакторной аутентификации значительно
Мониторинг и реагирование в реальном времени	Анализ поведения пользователей и транзакционной активности в режиме реального времени, выявление инцидентов и блокировка подозрительных операций до их завершения посредством использования искусственного интеллекта и машинного обучения
Инфраструктурная устойчивость	Использование технологий резервирования, распределенных дата-центров и облачных сервисов в целях защиты от DDoS-атак, системных сбоев и других внешних угроз
Межбанковское взаимодействие	Обмена информацией о киберугрозах между финансовыми организациями, регуляторами и правоохранительными органами. Коллективная защита позволяет оперативно реагировать на новые формы атак и вырабатывать единые стандарты обеспечения безопасности

Таким образом, цифровизация играет фундаментальную роль в обеспечении кибербезопасности банков, формируя современную экосистему защиты, которая сочетает технологические, организационные и регуляторные меры. С одной стороны, цифровая трансформация открывает новые уязвимости, связанные с ростом атак на банковские сервисы, но с другой – предоставляет мощные инструменты для проактивного противодействия угрозам. В итоге именно цифровизация становится основой построения устойчивой и безопасной банковской инфраструктуры в условиях развития глобальной цифровой экономики.

### Библиографические ссылки

1. Digitalisation of finance. URL: <https://www.bis.org/bcbs/publ/d575.pdf> (date of access: 21.09.2025).
2. *Brown I., Mues C.* An Experimental Comparison of Classification Algorithms for Imbalanced Credit Scoring Data // *Expert Systems with Applications*. 2012. Vol. 39. P. 3446–3453.
3. Доклад для общественных консультаций «Использование больших данных в финансовом секторе и риски финансовой стабильности». URL: [https://www.cbr.ru/Content/Document/File/131359/Consultation\\_Paper\\_10122021.pdf](https://www.cbr.ru/Content/Document/File/131359/Consultation_Paper_10122021.pdf) (дата обращения: 21.09.2025).
4. Об утверждении Инструкции об управлении рисками при аутсорсинге : постановление Правления Национального банка Респ. Беларусь, 21 февр. 2024 г., № 62. URL: [https://www.nbrb.by/legislation/documents/pp\\_62-2024.pdf](https://www.nbrb.by/legislation/documents/pp_62-2024.pdf) (дата обращения: 21.09.2025).
5. Об утверждении Инструкции об организации корпоративного управления : постановление Правления Национального банка Респ. Беларусь, 8 янв. 2020 г., № 1. URL: [https://www.nbrb.by/Legislation/Documents/pp\\_1-2022.pdf](https://www.nbrb.by/Legislation/Documents/pp_1-2022.pdf) (дата обращения: 21.09.2025).