

**Ссылка для цитирования этой статьи:**

Ахмедова Х.А., Сулейманова А.М. Проблемы и риски в сфере карточного бизнеса Сбербанка // Human Progress. 2025. Том 11, Вып. 7. С. 11. URL: [http://progress-human.com/images/2025/Tom11\\_7/Akhmedova.pdf](http://progress-human.com/images/2025/Tom11_7/Akhmedova.pdf) DOI 10.46320/2073-4506-2025-7a-27.

## **ПРОБЛЕМЫ И РИСКИ В СФЕРЕ КАРТОЧНОГО БИЗНЕСА СБЕРБАНКА**

**Ахмедова Хадижат Абдалахатовна**  
старший преподаватель отделения СПО,  
Дагестанский государственный университет,  
г. Избербаш, Российская Федерация

**Сулейманова Аминат Мусаевна**  
кандидат экономических наук,  
доцент кафедры экономических и общеобразовательных дисциплин,  
Дагестанский государственный университет,  
г. Избербаш, Российская Федерация

**Аннотация.** В настоящее время наблюдается высокая активность российских банков в развитии системы электронных платежей, сокращение бумажной технологий. Быстрое развитие технологий бесконтактных платежей, мобильных приложений и виртуальных карт создаёт новые возможности и одновременно новые вызовы для коммерческих банков.

В данной статье рассматриваются актуальные проблемы и риски, с которыми сталкивается Сбербанк в сфере карточного бизнеса. Основное внимание уделяется анализу основных вызовов, возникающих в процессе эмиссии и обслуживания банковских карт, а также оценке потенциальных угроз финансовой безопасности.

Авторы исследуют такие аспекты, как мошенничество, кибератаки, регуляторные риски и конкуренция на рынке платёжных услуг. Особое внимание уделяется методам минимизации выявленных рисков и стратегиям повышения безопасности платёжных операций.

**Ключевые слова:** карточный бизнес, пластиковые карты, безналичные расчёты, конкуренция, мошенничество, киберпреступность, технологическая инфраструктура, инновационные сервисы, качество обслуживания клиентов.

Карточный бизнес является одним из ключевых направлений деятельности Сбербанка, обеспечивая значительную долю комиссионных доходов и формируя основу для развития экосистемы банка. В 2024 году, несмотря на уверенное лидерство на российском рынке

банковских карт и положительную динамику основных показателей, Сбербанк сталкивается с рядом существенных проблем и рисков, требующих системного анализа и проактивного управления.

Комплексное понимание этих вызовов необходимо для разработки эффективных стратегий развития карточного бизнеса в условиях меняющейся рыночной конъюнктуры и технологической трансформации финансового сектора.

С ростом доли цифровых карт в общем объеме эмиссии до 42% в 2024 году Сбербанк сталкивается с увеличением технологических рисков, связанных с безопасностью виртуальных карточных продуктов. По данным Сбербанка, количество попыток несанкционированного доступа к цифровым картам возросло на 37% по сравнению с 2023 годом, что требует постоянного совершенствования механизмов защиты.

Особую проблему представляют атаки методом социальной инженерии, которые в 2024 году стали причиной 68% всех случаев мошенничества с цифровыми картами. Традиционные методы защиты, основанные на технологических барьерах, оказываются недостаточно эффективными против таких атак, что требует развития комплексных систем мониторинга и образовательных программ для клиентов. Одновременно с традиционными психологическими способами воздействия используются цифровые сервисы – это мессенджеры, дипфейки и так далее. Заместитель председателя правления «Сбера» Станислав Кузнецов перечислил пять фраз и слов, которые часто используют телефонные аферисты. Это «ФСБ», «МВД», «Центральный банк», «безопасный счет», «сообщите код из СМС / данные карты / паспорта / СНИЛС». Актуальными схемами мошенничества все еще остаются звонки по телефону и в мессенджерах, в которых злоумышленники представляются сотрудниками правоохранительных органов и Центробанка и под разными предлогами просят перевести средства «на безопасный счет» [1]. Сотрудники офисов Банка совместно со службами кибербезопасности за 12 месяцев 2024 года сохранили более 13 млрд руб. на счетах клиентов в рамках предупреждения мошенничества согласно отчету Сбербанка.

По оценке Сбербанка, ущерб от телефонного мошенничества в 2024 году составил не менее 295 млрд руб. 2024 год оказался самым насыщенным по количеству и разнообразию преступлений. Так, в марте 2024 года было зафиксировано рекордное количество мошеннических звонков – 20 млн в сутки. К началу 2025 года цифра уменьшилась до 5 – 6 млн звонков в сутки. Специалисты фиксируют огромное количество рисков и угроз со стороны мошенников вплоть до террористических актов.

Ежедневно появляются новые сценарии мошенничества. Топ самых распространенных схем:

- кража аккаунтов в Telegram через поддельную премиум-подписку;
- кража учетных записей на портале «Госуслуг»;
- звонки от лица ведомств: ФСБ, МВД, Банк России и другие;
- звонки от имени руководителей с использованием дипфейк-симуляции голоса и видео;
- фейковые лотереи и конкурсы;
- фальсификация банковских операций и счетов на оплату;
- провокации на противоправные действия [2].

В условиях технологических санкций и ограничений доступа к зарубежным IT-решениям Сбербанк столкнулся с проблемой зависимости от иностранных компонентов в инфраструктуре обслуживания карт. По оценкам экспертов, около 23% критически важного программного обеспечения в процессинговых системах банка имеет иностранное происхождение, что создает риски для стабильности карточного бизнеса.

Процесс импортозамещения в карточном бизнесе требует значительных инвестиций и времени. В 2024 году Сбербанк направил более 12 млрд рублей на разработку собственных технологических решений для процессинга, однако полное замещение иностранных компонентов ожидается не ранее 2026 года. Продолжается работа по замещению иностранных вендоров, баз данных и серверов. Полностью завершен отказ от 6 зарубежных вендоров, Завершен отказ от 22 вендорских продуктов. Полное завершение отказа от иностранного оборудования RISC-сервера, IBM DataPower, ORACLE Exadata. 90% всех СУБД – производства Сбера.

Традиционное доминирование Сбербанка на рынке банковских карт подвергается все более серьезным испытаниям со стороны финтех-компаний и цифровых банков, при этом основное давление оказывали Тинькофф Банк, Альфа-Банк и ВТБ [3]. Конкуренты активно внедряют инновационные продукты и сервисы, часто опережая Сбербанк по скорости вывода на рынок новых решений. По данным исследования Frank RG, среднее время запуска нового карточного продукта у Сбербанка составляет 7,5 месяцев, в то время как у Тинькофф Банка – 4,2 месяца [4].

В 2024 году наблюдается ускорение тренда на отказ от физических карт в пользу альтернативных платежных инструментов, особенно среди молодежной аудитории. По данным опросов, 42% клиентов в возрасте 18 – 25 лет предпочитают использовать мобильные платежные сервисы без привязки к физической карте, что создает риски снижения релевантности традиционных карточных продуктов.

Также отмечается рост популярности Системы быстрых платежей (СБП) как альтернативы карточным платежам в сегменте С2В-переводов. В 2024 году через СБП было проведено 27 % от общего объема розничных платежей, что существенно влияет на доходность эквайрингового бизнеса Сбербанка [6].

В 2024 году произошло ужесточение требований к обработке персональных данных держателей карт, что потребовало от Сбербанка значительных инвестиций в модернизацию систем хранения и обработки данных. Новые регуляторные требования привели к увеличению операционных расходов на обслуживание карточного портфеля.

В условиях постоянно растущей нагрузки на процессинговые системы и увеличения количества транзакций Сбербанк сталкивается с проблемой обеспечения бесперебойности карточной инфраструктуры.

Одним из ключевых стратегических вызовов для Сбербанка является определение оптимального баланса между развитием физических и цифровых карточных продуктов. С одной стороны, цифровые карты имеют более низкую себестоимость и высокую рентабельность. С другой стороны, исследования показывают, что физические карты остаются важным элементом брендинга и клиентского опыта, особенно в премиальном сегменте.

Несмотря на значительные успехи в развитии экосистемы, Сбербанк сталкивается с проблемами эффективной интеграции карточных продуктов с другими элементами экосистемы. Только 37% держателей карт Сбербанка регулярно используют три и более сервиса экосистемы, что существенно ниже целевого показателя [5].

В 2024 году наблюдается существенная трансформация методов мошенничества в сфере карточного бизнеса. Традиционные виды мошенничества (скимминг, фишинг) уступают место более сложным схемам, включающим комбинированные атаки с использованием методов социальной инженерии, глубоких фейков и компрометации данных аутентификации.

Активное внедрение биометрических технологий в карточные продукты Сбербанка (Face Pay, голосовая биометрия) создает новый класс рисков, связанных с возможностью компрометации биометрических данных. В отличие от пароля или ПИН-кода, биометрические характеристики невозможно изменить в случае их компрометации, что создает долгосрочные риски для безопасности [6]. В 2024 году были зафиксированы первые случаи успешных атак на системы биометрической аутентификации с использованием синтезированных глубоких фейков, что потребовало экстренного обновления алгоритмов распознавания и внедрения дополнительных механизмов защиты [7].

Карточный бизнес Сбербанка в 2024 году сталкивается с комплексом взаимосвязанных проблем и рисков, обусловленных как внешними факторами (регуляторное давление, усиление конкуренции, изменение потребительских предпочтений), так и внутренними вызовами (технологическая трансформация, операционная эффективность, стратегическое позиционирование). Эффективное управление этими рисками требует системного подхода, включающего технологические инновации, оптимизацию бизнес-процессов, совершенствование риск-менеджмента и гибкую адаптацию стратегии развития к меняющимся условиям рынка.

### Список литературы

1. В Сбербанке раскрыли гибридные схемы, которые используют мошенники. URL: <https://www.rbc.ru/life/news/673ed65c9a79475a872af025>.
2. Мошенники украли у россиян не менее 295 млрд руб. URL: <https://www.rbc.ru/life/news/67c701169a79471c14b76fa5>.
3. Рынок банковских карт России: итоги 2024 года // Frank RG. – М., 2024. – 145 с.
4. Рынок банковских услуг в России. URL: Frank RG. com.
5. Экосистемы в России: как развиваются и что ждет рынок. URL: <https://www.kommersant.ru/doc/6267515>.
6. Обзор основных типов компьютерных атак в финансовой сфере в 2024 году. URL: [https://cbr.ru/analytics/nps/sbp/1\\_2024/Банк России](https://cbr.ru/analytics/nps/sbp/1_2024/Банк России). – М., 2024.
7. Как мошенники научились подтверждать личность в банке. Всё оказалось проще... URL: <https://habr.com/ru/articles/791074/>

## PROBLEMS AND RISKS IN THE FIELD OF SBERBANK CARD BUSINESS

**Akhmedova Khadizhat Abdalakhmatovna**

Senior Lecturer at the Secondary Vocational Education Department,  
Dagestan State University,  
Izberbash, Russian Federation

**Suleymanova Aminat Musaevna**

PhD in Economics,  
Associate Professor of the Department of Economic and General Education Disciplines,  
Dagestan State University,  
Izberbash, Russian Federation

**Abstract.** Currently, there is a high level of activity among Russian banks in developing electronic payment systems and reducing the use of paper-based technologies. The rapid development of contactless payment technologies, mobile applications, and virtual cards creates new opportunities and challenges for commercial banks.

This article explores the current issues and risks faced by Sberbank in the field of card business. The focus is on analyzing the main challenges that arise during the issuance and maintenance of bank cards, as well as assessing potential threats to financial security.

The authors examine aspects such as fraud, cyberattacks, regulatory risks, and competition in the payment services market. Special attention is paid to methods of minimizing identified risks and strategies for improving the security of payment transactions.

**Keywords.** card business, plastic cards, cashless payments, competition, fraud, cybercrime, technological infrastructure, innovative services, and customer service quality.

### References

1. Sberbank has revealed hybrid schemes used by fraudsters. URL: <https://www.rbc.ru/life/news/673ed65c9a79475a872af025>.
2. Fraudsters stole at least 295 billion rubles from Russians. URL: <https://www.rbc.ru/life/news/67c701169a79471c14b76fa5>.
3. Russian bank card market: the results of 2024 // Frank RG. – M., 2024. – 145 p.
4. The banking services market in Russia. URL: Frank RG. com.
5. Ecosystems in Russia: how the market is developing and what awaits it. URL: <https://www.kommersant.ru/doc/6267515>.
6. An overview of the main types of computer attacks in the financial sector in 2024. URL: [https://cbr.ru/analytics/nps/sbp/1\\_2024/Bank of Russia, Moscow, 2024.7](https://cbr.ru/analytics/nps/sbp/1_2024/Bank of Russia, Moscow, 2024.7).
7. How fraudsters learned to verify their identity in a bank. Everything turned out to be easier... URL: <https://habr.com/ru/articles/791074>.