

УДК 338.001.36

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ БЕЗНАЛИЧНЫХ РАСЧЕТОВ

Воронцова А.С., студент гр. ЭБ-31, III курс
Поволжский государственный технологический университет
г. Йошкар-Ола

Современная экономика активно переходит на безналичные формы расчетов, что связано с удобством, скоростью и снижением затрат на проведение платежных операций. Однако вместе с ростом безналичных платежей увеличиваются и риски, связанные с мошенничеством, киберугрозами и недостатками в регулировании. Данная статья направлена на выявление основных угроз экономической безопасности безналичных расчетов и анализ эффективности применяемых методов защиты.

По данным Центрального банка РФ, доля безналичных платежей в общем объеме операций за последние 10 лет увеличилась с 45% до 85% (таблица 1). Основными драйверами этого роста являются цифровизация финансовых услуг, развитие мобильных приложений и внедрение технологий NFC. Однако, согласно отчету Ассоциации российских банков, с ростом доли безналичных расчетов увеличивается и количество киберпреступлений, связанных с банковскими картами и онлайн-платежами.

Таблица 1 . Динамика роста безналичных расчетов в России, 2015–2024 гг.

Год	Доля безналичных платежей (%)	Количество киберпреступлений (тыс.)
2015	45	120
2017	55	180
2019	65	250
2021	75	320
2023	83,4	390
2024	85	450

Источник: Центральный банк РФ [1], Ассоциация российских банков [3].

На основе анализа данных Федеральной службы по техническому и экспортному контролю (ФСТЭК) и Центрального Банка РФ (ЦБ РФ) можно выделить несколько ключевых угроз:

- Фишинг и социальная инженерия, включающие мошеннические схемы, направленные на получение персональных данных пользователей.
- Мошенничество с банковскими картами, которые включают скимминг, кардинг, компрометацию реквизитов.
- Кибератаки на платежные системы, содержащие DDoS-атаки, внедрение вредоносного ПО.
- Регуляторные и правовые риски, вызванные недостаточной правовой защитой пользователей и несовершенством законодательства в сфере кибербезопасности.

В ходе исследования были проанализированы статистические данные о киберпреступлениях, связанных с безналичными платежами (таблица 2). В 2024 году количество атак на банковские системы выросло на 22% по сравнению с 2023 годом, при этом около 42% инцидентов связаны с фишинговыми атаками.

Таблица 2. Динамика роста числа кибератак на финансовый сектор.

Год	Количество атак (тыс.)	Рост атак (%)
2021	320	-
2023	390	22
2024	450	15

Источник: ФСТЭК России [2].

Рост атак связан с увеличением числа пользователей безналичных платежей, развитием технологий автоматизации атак и расширением сетей киберпреступников. Повышенная цифровизация услуг также открывает новые векторы атак, такие как компрометация мобильных платежных приложений и атаки на цифровые кошельки.

Можно сделать вывод о том, что динамика роста кибератак на финансовый сектор подтверждает необходимость усиленной защиты платежных систем, внедрения более совершенных механизмов обнаружения мошенничества и повышения финансовой грамотности пользователей.

Рассмотрим, какую долю от общего числа кибератак занимают отдельные виды угроз для экономической безопасности страны (таблица 3).

Таблица 3. Распределение типов киберугроз в безналичных расчетах (2024 г.)

Тип угрозы	Доля от общего числа атак (%)
Фишинг	42
Вредоносное ПО	25
DDoS-атаки	18
Компрометация данных карт	15

Источник: ФСТЭК России [2], ЦБ РФ [1].

Из приведенных данных видно, что основную угрозу представляют фишинговые атаки, составляющие 42% от общего числа атак. Вредоносное ПО и DDoS-атаки также занимают значительную долю, что подтверждает необходимость усиления защиты платежных систем на уровне как пользователей, так и финансовых организаций.

На основе анализа угроз можно выделить несколько ключевых мер по защите безналичных расчетов:

– Развитие адаптивных систем мониторинга на основе использования искусственного интеллекта и машинного обучения для выявления подозрительных операций в реальном времени.

– Многофакторная аутентификация (MFA), включающая в себя внедрение биометрической аутентификации и динамических паролей для повышения уровня защиты.

- Токенизация платежных данных, представляющая собой применение временных цифровых идентификаторов вместо хранения реальных данных карт.
- Разработка программ по информированию населения о новых видах угроз и методах их предотвращения.
- Введение новых стандартов безопасности для банков и платежных сервисов, например, расширение требований PCI DSS.

Анализ показал, что безналичные расчеты несут в себе значительные риски, связанные с киберугрозами и мошенничеством. Однако использование современных технологий защиты, таких как адаптивные системы мониторинга, многофакторная аутентификация и токенизация данных, позволяет минимизировать данные угрозы. Важным направлением является повышение информационной грамотности пользователей, а также дальнейшее совершенствование регуляторной базы.

Список литературы

1. Центральный банк Российской Федерации. Отчет о развитии национальной платежной системы за 2024 год. – М.: Центробанк РФ, 2024. URL: <https://cbu.ru/statistics/nps/psrf/>
2. Федеральная служба по техническому и экспортному контролю России. Анализ угроз информационной безопасности финансового сектора. – М.: ФСТЭК России, 2024. URL: <https://bdu.fstec.ru/threat-section>
3. Международный стандарт PCI DSS: требования к защите платежных данных. – М.: Международный совет по стандартам безопасности, 2024. URL: <https://www.pcisecuritystandards.org/>
4. Родионова Е. В. ESG - трансформация банковского сектора России // Экономическое развитие России: вызовы и возможности в меняющемся мире: Материалы Международной научно - практической конференции. Краснодар: Кубанский государственный университет, 2023. С.209-213