УДК 336.7

Р. А. Ступаченко, А. А. Толстиков,
факультет экономики, менеджмента, сервиса и туризма,
Омский государственный педагогический университет
Научный руководитель: канд. экон. наук, доц. А. А. Романова

Скимминг и мошенничество с банковскими картами: современные методы и правила защиты

Аннотация. В статье представлены результаты работы по вычислению распространенных способов мошенничества в Российской Федерации, а также актуальных универсальных способов защиты от них.

Ключевые слова: мошенничество, банковские карты, скимминг, вишинг, фишинг.

Мошенничество с банковскими картами в Российской Федерации (РФ) является самым распространенным видом мошенничества. С апреля по июнь 2025 г., по данным Центрального банка РФ, банки отразили 38 700 000 попыток мошеннических атак. Это на 150 % больше, чем в предшествующих четырех кварталах [2]. При этом размер ущерба сократился на 15,9 % по сравнению с соответствующими предыдущими четырьмя кварталами (табл.).

Данные за II квартал 2025 года

Показатель	Результат	Процентное соотношение
Отражено мошеннических атак	38,7 млн	+150 %
Предотвращено ущерба	3,4 трлн руб.	–15,9 %
Реальный ущерб	6,3 млрд руб.	

Скимминг представляет собой технологию несанкционированного сбора данных банковской карты с целью их дальнейшего использования для изготовления подделки. Традиционный скимминг осуществляется путем физического контакта карты со скимминг-устройством, которое злоумышленники тайно устанавливают на банкоматы или платежные терминалы. Для маскировки эти незаконные модули часто выполняются в том же цвете и стиле, что и легальное оборудование, что затрудняет их визуальное обнаружение. Помимо основного корпуса, скиммер может включать в себя накладную клавиатуру, которая перехватывает вводимые пин-коды. Злоумышленники предпочитают устанавливать такие устройства в местах с низкой проходимостью или в вечернее время, чтобы избежать разоблачения. Собранные данные либо передаются по беспроводной связи, либо сохраняются во внутренней памяти для последующего извлечения. В результате владелец карты может долгое время не подозревать о компрометации своих реквизитов.

Следующий вид мошенничества связан со звонками по телефону. Эта целая категория, включающая в себя различные методы, называется вишингом. Чаще всего мошенники звонят под видом сотрудников банка и с помощью навыков социальной инженерии убеждают жертву срочно перевести все средства на «специальный защитный» или «временный» счет, который на самом деле контролируется самим мошенником. Опасность данного вида заключается в том, что он является очень гибким, и преступники постоянно придумывают новые способы обмана.

Одним из по-прежнему активно функционирующих видов мошенничества является фишинг. Данный вид мошенничества направлен на хищение личных данных с помощью фальшивых веб-ресурсов, дизайн которых в точности скопирован у настоящих, и рассылки сообщений, имитирующих официальные коммуникации от банков, платежных систем, государственных порталов и торговых площадок. Когда пользователь вводит на таком сайте реквизиты карты, она немедленно перехватывается преступниками для последующего незаконного списания средств. За последние несколько лет многие люди перешли на оплату услуг и товаров по QR-коду. Злоумышленники используют следующий метод: они заменяют легитимные QR-коды фальшивыми, подменяя платежные реквизиты.

Основные мероприятия по защите от мошенничества представляют собой в первую очередь проверку устройства перед использованием

на наличие посторонних или подозрительных накладок, проверку места, куда вставляется карта, а также закрытие клавиатуры во время ввода пароля. При оплате в торговых точках стоит выбирать операцию с чипом, а не с магнитной полосой. Снимать наличные рекомендуется в банкоматах, расположенных внутри отделений банков или в хорошо охраняемых местах. Риск установки скиммеров на таких устройствах ниже, чем на уличных банкоматах. Второе правило — ни при каких обстоятельствах не разглашать конфиденциальные данные, так как легитимные организации никогда не запрашивают эти данные по телефону или в письмах. Третье правило — все финансовые операции нужно совершать только через официальные сайты и приложения, установленные с ресурсов самой кредитной организации. Перед оплатой через QR-код в общественных местах нужно удостовериться в его подлинности, например, посредством сравнения реквизитов QR-кода с чеком организации [1].

1. «Карта, я тебя знаю». Что такое скимминг и как с ним бороться // СберСова : [сайт]. — 2021. — 18 окт. — URL: https://sbersova.ru/sections/protection/karta-ya-tebya-znayu-chto-takoe-skimming-i-kak-s-nim-borotsya (дата обращения: 28.09.2025).

2. Противодействие мошенническим операциям: итоги II квартала // Центральный Банк России : [сайт]. — 2025. — 7 авг. — URL: https://www.cbr.ru/press/event/?id=26832 (дата обращения: 28.09.2025).