УДК 336.719

НЕРЕЛЕВАНТНЫЙ УРОВЕНЬ ФИНАНСОВОЙ ГРАМОТНОСТИ НАСЕЛЕНИЯ КАК ФАКТОР РОСТА МОШЕННИЧЕСТВА В ФИНАНСОВОЙ СФЕРЕ

Куварин Д. Ю.

студент,

Кубанский государственный аграрный университет имени И.Т. Трубилина, Краснодар, Россия

Зиниша О. С.

к.э.н., доцент

Кубанский государственный аграрный университет имени И.Т. Трубилина, Краснодар, Россия

Кочеян Д.Г.

студент,

Кубанский государственный аграрный университет имени И.Т. Трубилина, Краснодар, Россия

Аннотация

В настоящей статье рассматривается взаимосвязь уровня финансовой грамотности и мошенничества в финансовой сфере. Выявлены основные схемы мошенников в области использования банковских карт, а также разработаны основные методы противодействия их деятельности. Результаты проведенного исследования способствуют разработке механизмов совершенствования противодействия мошеннических операций в области предоставления финансовых услуг с использованием информационно-телекоммуникационных технологий.

Ключевые слова: финансовая грамотность, мошенничество, банковский бизнес, информационно-телекоммуникационные технологии.

IRRELEVANT LEVEL OF FINANCIAL LITERACY OF THE POPULATION AS A FACTOR IN THE GROWTH OF FRAUD IN THE FINANCIAL SECTOR

Kuvarin D. Yu
student
Kuban State Agrarian University named after I.T. Trubilin
Krasnodar, Russia

Zinisha O. S.
Cand. Econ. Sci.
associate professor of the department of monetary circulation and credit
«Kuban State Agrarian University named after I.T. Trubilin»
Krasnodar, Russian Federation

Kocheyan D.G.
student
Kuban State Agrarian University named after I.T. Trubilin
Krasnodar, Russia

Abstract.
This article examines the relationship between the level of financial literacy and fraud in the financial sector. The main schemes of fraudsters in the field of using bank cards have been identified, and the main methods of countering their activities have been developed. The results of the study contribute to the development of mechanisms for improving the fight against fraudulent transactions

in the provision of financial services using information and telecommunications technologies.

Keywords: financial literacy, fraud, banking, phishing, credit cards, information and telecommunications technologies

Финансовая грамотность – это способность понимать, как работают деньги в мире, и принимать обоснованные, а также разумные решения в отношении всей финансовой деятельности [9]. Человек, обладающий финансовой грамотностью, знает, как зарабатывать, управлять и инвестировать деньги. Он знаком с финансовыми продуктами и применяет свои знания, чтобы наилучшим образом их использовать. Последние события в мире сделали финансовое образование и осведомленность все более важными [2]. Отсутствие знаний о широком спектре доступных финансовых инструментов может привести к неправильному принятию решений и к дорогостоящим ошибкам.

В 2020 году, по заказу Банка России, Институт фонда «Общественное мнение» (ФОМ) провел третий этап замера уровня финансовой грамотности населения Российской Федерации [5].

Значение индекса финансовой грамотности по направлениям финансовых знаний, финансового поведения, финансовой устойчивости представлено на рисунке 1.

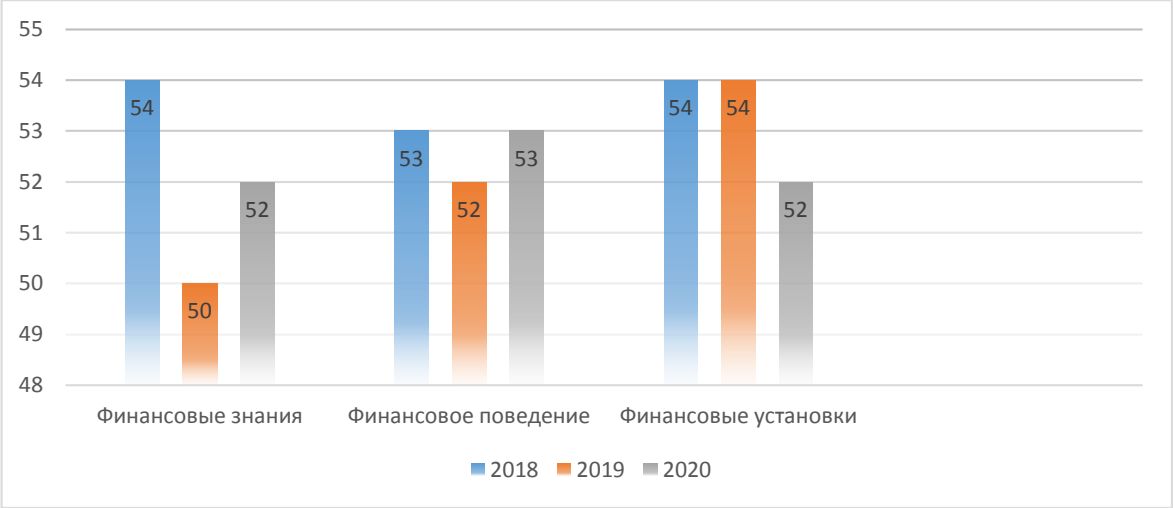

Рисунок 1 – Динамика значений субиндексов финансовой грамотности населения в России, балл. [5]

Анализируя данные опроса, можно прийти к выводу, что финансовые знания остались на прежнем уровне, но вырос уровень финансового поведения, что является отражением увеличения денежных средств населения, отложенных на «черный день»; также выросла доля граждан, которые осведомлены, какие организации занимаются защитой прав потребителей на финансовом рынке: с 38% до 50%.

Общее значение итогового индекса финансовой грамотности в 2020 году достигло 54 пункта, что на 2 пункта выше показателя 2017 года [5].

С ростом цифровизации финансовых услуг и использования безналичных платежей, прежде всего на основе пластиковых карт, в последние годы наблюдается увеличение объема мошеннических действий, которые обходятся экономике в убытки, оцениваемые в миллиарды долларов [1]. Особенно растет количество мошеннических действий в отношении потребителей финансовых услуг, к которым относятся несанкционированный доступ к чужому банковскому счету или реквизитам платежной карты для осуществления мошеннических транзакций.

Следует отметить высокую степень изощренности, с которой совершается мошенничество с потребителями, в результате чего многие мошеннические действия остаются нераскрытыми, а потерпевшие не получают справедливую компенсацию [8]. Например, мошенничество с авторизованными платежами push, мошенничество с бесконтактными картами и скиммингом карт, - и это лишь некоторые из них, - являются новыми видами мошенничества, которые могут беспрепятственно продолжаться в течение длительного времени, если их вообще обнаружат. Системы обнаружения и проверки мошенничества банков могут пропускать незаконные транзакции, которые кажутся подлинными; поэтому банки уделяют особое внимание транзакциям своих клиентов, чтобы выявлять и сообщать о любых мошеннических действиях с их счетами [3].

Данные по количеству кредитных карт, эмитированных российскими кредитными организациями, представлены на рисунке 2.

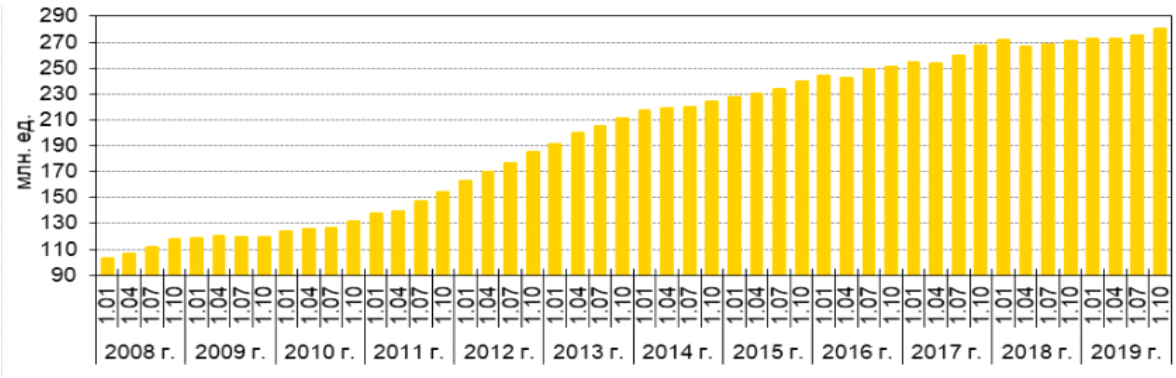

Рисунок 2 – Количество расчетных и кредитных карт, эмитированных кредитными организациями в России, ед. [5]

Данные рисунка 2 показывают, что с начала 2008 года по 2019 год объем эмитированных кредитных карт вырос на 300%, и достиг отметки в 280 миллионов единиц. Данные количественные изменения привлекли большое количество мошенников, стремящихся заполучить денежные средства владельцев данных карт.

По данным ФКУ «Главный информационно-аналитический центр» МВД России только за период с января по март 2021 года было зафиксировано 85 031 преступлений в области осуществления мошенничества, причем, около 65% преступлений было совершено с использованием информационно-телекоммуникационных технологий (ИКТ) [6]. Это означает, что данное направление деятельности для мошенников является особенно приоритетным.

Следует отметить, что для ряда потребителей финансовых услуг банковская карта оказалась «навязанным» финансовым инструментом [5]. Многие учреждения и организации стали перечислять заработную плату сотрудникам на банковские карты, выданные в рамках корпоративных проектов, потом к безналичному обслуживанию подключился Пенсионный фонд РФ, и на карточные счета стали зачислять пенсии.

Основная проблема использования банковских карт заключается в том, что многие организации пренебрегают осуществлением мероприятий, направленных на повышение уровня осведомленности своих клиентов и сотрудников о правилах безопасности при использовании банковских карт [7].

Основная задача деятельности злоумышленников - это получение различного рода информации, которая включает данные о банковских реквизитах, паспортные данные владельца и другая информация.

Мошенник использует различные ухищрения для получения информации о банковской карте, но в большинстве случаев сами владельцы данных карт передают эту информацию по своей доверчивости и невнимательности.

Рассмотрим основные мошеннические модели получения данных о банковских картах и методы их противодействия в таблице 1.

Таблица 1 –Основные мошеннические модели с банковскими картами (составлено авторами)

Наименование мошеннической модели	Особенности реализации данной схемы	Методы противодействия
Скимминг – кража данных карты при помощи специального считывающего устройства	Сущность скимминга заключается в хищении информации о банковской карте через специальное считывающее устройство (скиммер), которое вмонтировано в банкомат . Данное устройство считывает номера карт и другую информацию о кредитных и дебетовых картах, сохраняя ее для передачи преступникам Помимо этого, злоумышленники могут установить скрытые камеры совместно с накладной клавиатурой, которые активируются при вводе данных клиентом банка. Данная информация мгновенно передается злоумышленникам, которые используют ее по своему усмотрению.	1) Необходимо выбирать только проверенные банкоматы, расположенные в отделениях банка; 2) Перед использованием банкомата необходимо проверить его на наличие встроенной клавиатуры, скиммера, а также скрытой камеры. 3) Никому не сообщайте PIN – код от вашей банковской карты; 4) Необходимо подключить услугу «мобильный банк» и услугу sms-сообщения об операциях по карте с целью повышения уровня контроля за движением средств по данному счету. 5) Используйте банкоматы, оснащенные антискимминговыми накладками и джиттерами 6) Используйте карты с технологией NFC 7) При вводе PIN – кода прикрывайте рукой вводимые числа
Фишинг - это форма мошенничества, при которой злоумышленник маскирует свою деятельность под официальное юридическое или физическое лицо в электронной переписки или в других формах общения	Фишинговые атаки обычно основаны на методах социальных сетей, применяемых к электронной почте или другим методам электронной связи. Некоторые методы включают прямые сообщения, отправленные через социальные сети, и текстовые сообщения SMS, чтобы обманом заставить жертв разглашать личную и финансовую информацию, такую как пароли, идентификаторы учетных записей или данные кредитных карт.	Чтобы предотвратить попадание фишинговых сообщений к конечным пользователям, эксперты рекомендуют многоуровневые меры безопасности, в том числе: - антивирусное программное обеспечение; - как настольные, так и сетевые брандмауэры; - антишпионское программное обеспечение; - панель инструментов антифишинга (устанавливается в веб-браузерах); - фильтр электронной почты шлюза; - шлюз веб-безопасности; - фильтр спама; и фишинговые фильтры от таких поставщиков, как Microsoft.
Вишинг – это один из распространенных видов фишинга, основанного на использовании	Сущность вишинга заключается в том, что злоумышленник, используя телефонную коммуникацию представляются сотрудником банка, который использует различные методы психологического	1) Никому не сообщайте пин-код карты. Помните, сотрудники банка не вправе требовать такие данные. 2) Никогда не отправляйте в одном электронном сообщении все персональные данные банковской

социальной инженерии.	манипулирования с целью заполучения конфиденциальной информации или подталкивают к совершению определенных действий, направленных на получение данной информации.	карты (номер, срок действия, CVC-код). 3) Не сообщайте логин и пароль от личного кабинета банка.

Таким образом, по итогам проведенного авторами исследования, можно сформулировать следующие выводы о том, что виды мошенничества в сфере предоставления финансовых услуг становятся все более сложными по своей природе и распространенности на различные финансовые институты. Основным фактором роста уровня мошенничества является низкий уровень финансовой грамотности населения.

Мошенничество является серьезной проблемой для всей индустрии финансовых услуг, которая растет с ростом популярности электронных денежных операций. Для эффективного предотвращения преступных действий, которые приводят к утечке информации о банковских счетах, скимингу, подделке кредитных карт, краже миллиардов долларов ежегодно и потере репутации и лояльности клиентов, эмитенты кредитных карт должны рассмотреть возможность внедрения передовых методов предотвращения мошенничества с кредитными картами и выявления мошенничества [3]. Методы, основанные на машинном обучении, могут постоянно повышать точность предотвращения мошенничества на основе информации о поведении каждого владельца карты.

В этом контексте Стратегия повышения финансовой грамотности Российской Федерации на 2017-2023 годы нацелена на разработку и внедрение программ и методов интерактивного обучения, в первую очередь, для студентов и школьников с использованием различных цифровых образовательных ресурсов [4]. Целью данной стратегии является внедрение в практику новых методов и форм финансового образования, основанных на передовых информационно - коммуникационных технологиях.

Библиографический список:

1. Жданова, О. А. Финансовое мошенничество в современном мире / О. А. Жданова, Ю. В. Лабовская, И.Ф, Дедюхина // Государственная служба и кадры. – 2020. - № 4. – С. 97.

2. Меньшенина, Т. Б. Финансовая грамотность населения как фактор экономического развития государства/ Т. Б. Меньшенина, В. И. Гуштан // Стратегии развития социальных общностей, институтов и территорий. – 2019. - № 1 – С. 44.

3. Зиниша, О. С. Мероприятия Банка России по противодействию нелегальной деятельности участников отечественного финансового рынка / О. С. Зиниша, Д. Г. Кочеян, В. Н. Иванов // Валютное регулирование. Валютный контроль. - 2021. - №2. - С. 20-25.

4. Об утверждении Стратегии повышения финансовой грамотности в Российской Федерации на 2017-2023 гг.: распоряжение Правительства Российской Федерации № 2039-р от 25 сентября 2017 г. // КонсультантПлюс: Версия Проф. – Справ.-прав. система.

5. Официальный сайт Центрального банка Российской Федерации (Банка России) [Электронный ресурс]. - Режим доступа: http://www.cbr.ru/(дата обращения: 18.12.2020).

6. Официальный сайт Министерства внутренних дел Российской Федерации [Электронный ресурс]. - Режим доступа: https://мвд.рф// (дата обращения: 13.05.2021).

7. Теплова, Д. Криминологические основы противодействия организованному мошенничеству: монография / Д. Теплова. – М.: Мир, 2018. -285 с.

8. Шейнов, В. П. Как защититься от обмана и мошенничества: монография / В. П. Шейнов. - М.: Харвест, 2019. – 406 с.

9. Dennis Philip (2021). Financial literacy and fraud detection [Электронный ресурс]. – Режим доступа:

https://www.researchgate.net/publication/351119529_Financial_literacy_and_fraud_detection (дата обращения: 14.05.2021).

Оригинальность 93%