

DOI: 10.19181/population.2022.25.1.3

ФИНАНСОВОЕ МОШЕННИЧЕСТВО В ПЕРИОД ПАНДЕМИИ COVID-19

Медведева Е. И.¹, Крошилин С. В.^{1,2*}

¹Институт социально-экономических проблем народонаселения ФНИСЦ РАН
(117218, Россия, Москва, Нахимовский проспект, 32)

²Рязанский государственный медицинский университет имени академика
И. П. Павлова (390026, Россия, Рязань, ул. Высоковольтная, 9)

*E-mail: krosh_sergey@mail.ru

Для цитирования:

Медведева Е. И., Крошилин С. В. Финансовое мошенничество в период пандемии COVID-19// Народонаселение. – 2022. – Т. 25. – № 1. – С. 29-42. DOI: 10.19181/population.2022.25.1.3.

Аннотация. Целью настоящего исследования являлось изучение новых способов финансового мошенничества, с которыми столкнулось российское общество в период пандемии. Объект исследования — российский социум, предмет — схемы финансового мошенничества, которые стали возможным благодаря ограничительным мерам и бурному развитию интернет-торговли в период пандемии. Современное общество сталкивается с различными вызовами, которые обусловлены не только прогрессивными технологиями развития, инновациями, сменой технологических укладов, повсеместным внедрением цифровых технологий, но и с факторами, появление которых было сложно предсказать — пандемия COVID-19. Прошло два года как весь мир живёт в условиях пандемии, но за это время поведенческие установки социума претерпели значительные изменения: от «режима самоизоляции» и обязательного «ношения» масок — до работы на «удалёнке» и обязательного предъявления QR-кодов. Последние изменения в значительной степени предопределили бурное развитие информационно-коммуникационных технологий, которые повлияли на реальное общение и возможности изменения онлайн поведения: покупки, получение справок и документов, работа на «удалёнке» охватили от 50 до 80% работников в различных сферах. Уход в онлайн стал причиной не только повышенного спроса на коммуникационные услуги, развитие интернет-торговли, интернет-банкинга (в начале пандемии была впервые проведена сделка по ипотечному приобретению жилья в онлайн режиме), но способствовал созданию новых видов финансового мошенничества посредством коммуникационных технологий. В статье использованы материалы Росстата, ВЦИОМ, Банка России, аналитические материалы финансовых структур и результаты исследований, в том числе авторских, проведённых на юго-востоке Московской области. Результаты анализа могут быть актуальны и значимы для профилактики совершения мошеннических действий, а также при проведении занятий по финансовой грамотности населения. Соответствующие структуры власти, комитеты и комиссии могут воспользоваться данными материалами для проведения разъяснительных мероприятий для населения.

Ключевые слова: социально-экономические проблемы, социум, пандемия, коронавирус, финансовое мошенничество, электронная коммерция, информационные технологии

Развитие рыночной экономики, современных технологий, доступности большего числа товаров и услуг предопределило расширение в мире и России «общества потребления» [1]. Изменению парадигмы потребительского поведения способствует появление и интенсивное развитие новых форм торговли, в том числе посредством сети интернет. По оценке специалистов, в начале 2021 г. в социальных сетях зарегистрировалось почти полмиллиарда

пользователи проводят в Интернете 7 часов 17 минут каждый день. Больше всего они готовы тратить онлайн на «путешествия» (24 млрд долларов США), а средний размер онлайн-покупок потребительских товаров — 190 долларов США в год на человека². Только 39% пользователей интернета в России используют приложения для покупок (в мире — 66%), а банковские приложения в России более популярны — 45% (в мире — 35%) (рис. 1).

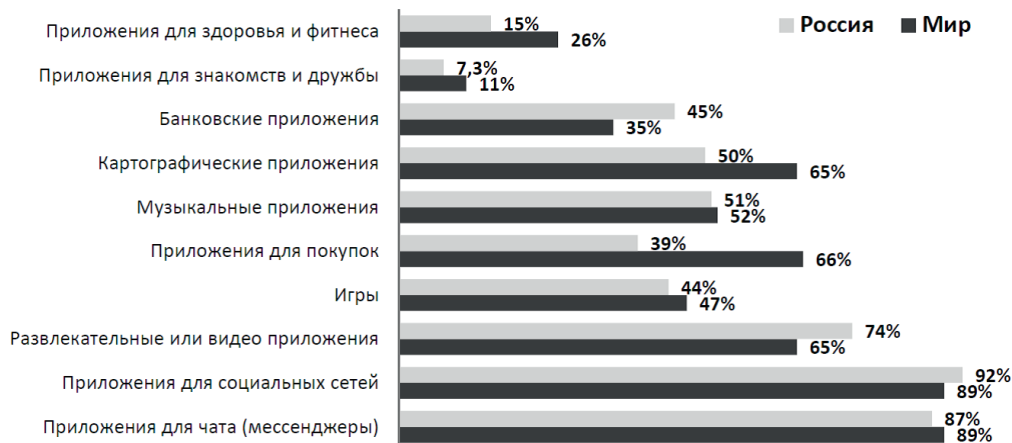


Рис. 1. Мобильные приложения в мире и России 2020 г., % от населения

Fig. 1. Mobile applications in the World and Russia 2020, % of the population

Источник: Вся статистика интернета и соцсетей на 2020 год — цифры и тренды в мире и в России // WebCanape: [сайт]. — URL: <https://datareportal.com/reports/digital-2021-global-overview-report> (дата обращения: 24.11.2021).

новых пользователей. Мобильным телефоном пользовались 8 млрд человек (66,6% мирового населения), а 95% жителей были в зоне покрытия сотовой связи. Уровень «проникновения» интернета составлял 59,5%; социальными сетями пользовались 53,6% мирового населения¹. В России 118 млн человек (81% россиян) пользуются интернетом (по данным Digital-2020). Больше половины (53%) предпочитают мобильный интернет. Численность аудитории социальных сетей в России на начало 2020 г. составила около 70 млн человек (48% населения). В среднем российские

В последние годы, в том числе в условиях пандемии, наблюдается стремительное увеличение пользователей Сети в России. «Вынужденная» необходимость предопределяет совершать всё больше действий онлайн. Перевод многих работников и учащихся на «удалёнку» также повлекли за собой стремительный рост подключения к интернету: те, кто был уже подключен, меняли тарифные планы, оборудование, для повышения скорости интернета. Повышение востребованности услуг предоставляемых в электронном виде, рост электронной коммерции (e-commerce) и количества операций

¹ Вся статистика интернета и соцсетей на 2021 год — цифры и тренды в мире и в России // WebCanape: [сайт]. — URL: <https://datareportal.com/reports/digital-2021-global-overview-report> (дата обращения: 24.11.2021).

² Global Digital 2021 // We Are Social and Hootsuite: [сайт]. — URL: <https://datareportal.com/reports/digital-2021-global-overview-report> (дата обращения: 24.11.2021).

с банковскими картами у населения (оплата онлайн), повлекли за собой увеличение объёма безналичных платежей совершаемых физическими лицами, и появлению новых торговых систем, обслуживающих клиентов через сеть интернет (например, практически все крупные торговые сети и магазины были вынуждены расширить свой ассортимент интернет-магазинов и/или открыть электронные торговые площадки, если их не было до пандемии).

На конец 2019 г. отсутствовал доступ к интернету у 24% российских домохозяйств, в сельской местности — у 43,5%. Компьютер отсутствовал у более трети (38,3%) российских семей, однако большинство его отсутствие компенсируют возможностями сотового телефона: последнего нет у 1,4% российских домохозяйств. В октябре 2020 г. премьер-министр России М. Мишустин заявил, что в ближайшие четыре года необходимо достичь уровня показателя «доступ в интернет» не менее 90% домохозяйств в России³.

³ Информационное общество в Российской Федерации. 2020: стат. сб. / Федеральная служба государственной статистики; Нац. исслед. ун-т «Высшая школа экономики». — Москва: НИУ ВШЭ, 2020. — С. 21.

В России в меньшей мере, чем в других странах, население использует интернет для приобретения товаров и услуг — 41% (для сравнения в США — 57%, во Франции — 67%, в Великобритании — 83%). Однако этот показатель составляет чуть меньше половины от подключений к интернету в России в целом. Женщины чаще пользуются интернетом для заказа товаров, чем мужчины. Если проанализировать возрастные группы, то в когорте 25–34 года больше половины (53,7%) используют интернет для совершения покупок (табл. 1). В 2019 г. чаще всего⁴ заказывали в интернете одежду, обувь и спортивные товары (57,6%), на втором месте — финансовые услуги (43,5%), на третьем — предметы домашнего обихода (27,0%), на четвёртом — телекоммуникационные услуги (26,9%), на пятом — билеты на развлекательные мероприятия (23,1%). В период пандемии количество заказов через интернет значительно увеличилось, особенно в период «жестких» ограничительных мер. Это выступило драйвером роста рынка электронной коммерции в России.

⁴ Там же.

Таблица 1
Доли групп населения, которые используют Интернет для покупки товаров и услуг, %
Table 1
The proportion of groups of the population who use the Internet to purchase goods and services, %

Пол, возраст	В % от общей численности населения			В % от численности населения, использующего Интернет		
	2015	2018	2019	2015	2018	2019
Мужчины	17,6	32,1	33,5	23,7	37,8	38,7
Женщины	21,3	37,0	37,7	29,3	44,7	44,4
15–24 года	25,0	45,3	44,2	26,1	46,3	44,9
25–34 года	31,4	53,1	53,7	34,0	54,6	55,1
35–44 года	23,8	43,7	45,1	28,2	46,2	47,3
45–54 года	14,9	31,9	34,5	21,4	36,5	38,2
55–64 года	7,5	16,1	18,2	17,0	23,3	25,0
65–74 года	2,3	5,6	7,1	11,4	13,8	15,3

Источник: Информационное общество в РФ2020: стат.сб. / Росстат; НИУ «Высшая школа экономики». — Москва : НИУ ВШЭ, 2020. — С. 103.

В 2021 г. Китай остался лидером в розничной торговле через Интернет-магазины: доля его продаж составила 52,1% (2779,3 млрд долларов США). На втором месте США — 19%, на третьем — Великобритания — 4,8%. Российская Федерация не входит даже в десятку лидеров по объёму электронной коммерции. Однако, растёт доля интернет-торговли в структуре ВВП России: в 2020 г. она увеличилась до 2,5% (1,3% в 2019 г.) [2]. Наблюдается высокая дифференциация регионов России по этому показателю, где ли-

дирует центральный федеральный округ.

Рынок интернет-торговли России делится на локальный сектор и трансграничный. На рисунке 2 приведена динамика показателей рынка электронной коммерции за время пандемии: 92% — темп роста внутреннего рынка интернет-торговли в «пик» карантинных мер; от общего объёма его доля составила 86%, а доля трансграничного рынка сократилась на 25% (449 млрд руб.) по сравнению с 2019 г. [2].

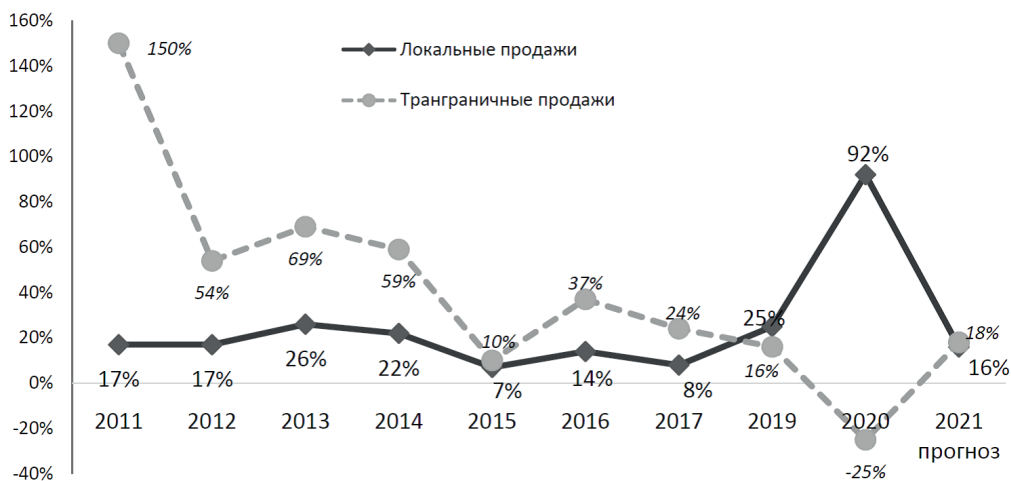


Рис. 2. Рост рынка электронной коммерции в России в 2011–20 гг. (2021 г. — прогноз),%

Fig. 2. The growth rate of the e-commerce market in Russia in 2011–20 (forecast 2021),%

Источник: построено по данным Statista «Year-on-year domestic and cross-border Russian e-commerce market growth rate from 2011 to 2020 with forecast till 2021»: [сайт]. — URL: <https://www.statista.com/statistics/1073320/russian-e-commerce-foreign-and-domestic-market-volume-growth/> (дата обращения: 27.10.2021).

В период жёсткого локдауна наблюдалось увеличение открытия новых онлайн ритейлеров. Это была вынужденная мера даже для тех компаний, которые работали в оффлайн формате. Можно выделить несколько основных факторов, которые способствовали развитию e-commerce в период пандемии⁵: во-первых, это «появление» новых покупателей (по оценки различных аналитиков за

период самоизоляции в российский сектор Интернета «пришло» около 10 млн новых покупателей). Во-вторых, удалённая занятость — по данным Росстата, по завершении пандемии порядка 5,7 млн человек продолжат работать на «удалёнке». Некоторые из них покинут «города работодателя» и будут вынуждены пользоваться интернет-магазинами и службами доставки. В-третьих, вынужденная изоляция. Старшее поколение, которому периодически «рекомендуют оставаться дома», выполняя предписания местных органов здравоохранения, и после сня-

⁵ Электронная коммерция в 2021 году. Как пандемия влияет на онлайн-рынок? // Digital агентство ADVIANA: [сайт]. — URL: <https://vc.ru/trade/243482-elektronnaya-kommerciya-v-2021-godu-kak-pandemiya-vliyaet-na-online-rynok> (дата обращения: 24.11.2021).

тия ограничений будут использовать заказы товаров из интернет-магазинов (как более удобный и безопасный способ потребления) с доставкой на дом.

Таким образом, пандемия коронавируса выступила драйвером роста электронной торговли и операций, которые совершались посредством оплаты банковскими карточками. Это способствовало росту мошеннических схем — их увеличению и «разнообразию». По оценке экспертов [3], если 10–15 лет назад около 90% краж осуществлялось «стандартным» способом и лишь 10% в электронном виде, то сегодня ситуация изменилась на противоположную: 9 из 10 финансовых махинаций осуществляются с помощью цифровых и/или интернет-технологий [4].

В условиях самоизоляции в связи с COVID-19 произошло ухудшение экономической ситуации, снижение реальных доходов населения, у некоторой части — потеря работы. Это стало причиной активизации деятельности мошенников именно в банковской сфере. Как показывает опыт, в период нестабильной ситуации в экономике растет число различных видов мошенничества. Например, за время валютного кризиса 2014–2015 гг. в среднем на треть выросло число мошенничеств с банковскими картами. По оценкам аналитиков, во время пандемии появились новые виды мошенничества⁶.

1. С началом пандемии поисковые запросы населения в Интернете были сконцентрированы на поиске информации о средствах защиты и лекарствах, что стало причиной предложения от мошенников о якобы эффективных и надёжных препаратах от коронавируса. Под видом надёжных лекарств предлагались обыкновенные препараты от лица ведущих фарм-компаний. В лучшем случае это влекло за собой только потерю денежных средств, в худшем — приобретение «псевдо-лекарств» становилось угрозой для здоровья людей.

⁶ Пандемия мошенничества, или шесть новых способов финансового обмана // ВашиФинансы.РФ: [сайт]. — URL: <https://vashifinancy.ru/for-smi/press/news/pandemiya-moshennichestva-ili-shest-novykh-sposobov-finansovogo-obmana/> (дата обращения: 24.11.2021).

2. Появление предложений в сети (электронные письма) о помощи в оформлении кредитных каникул и/или получении определённых пособий. Все ссылки в такой переписке ведут на сайты, где необходимо ввести данные банковской карты пользователя, чтобы оплатить комиссию за услугу. Это приводит к потере денежных средств посредством несанкционированного доступа к карте.

3. Оплата штрафа за нарушение режима самоизоляции от имени МВД или государственных органов — это ещё одна схема. Причём мошенников интересует лишь процедура оплаты, которую они и предлагают совершить на псевдо-сайтах. Подобный подход использовался не только в Интернете, но и на улице, когда предложение «оплатить штраф» на месте поступало от мошенников.

4. Рассылка электронных сообщений и/или звонков от имени врачей или Роспотребнадзора о том, что ваш родственник или друг госпитализирован с диагнозом «коронавирус». Предлагается перевести деньги на организацию лечения, оплату лекарств и тому подобное. Обычно просят сделать перевод денег по номеру телефона для «ускорения» процесса. Для предотвращения подобного необходимо позвонить в больницу, где якобы госпитализирован ваш знакомый или родственник.

5. В период пандемии со стороны мошенников участились атаки на неквалифицированных инвесторов, которым предлагается вложить собственные средства в фармацевтическую сферу. При этом обещают высокую доходность за счёт оперативного выхода на рынок противовирусных препаратов. В итоге это приводит к потере денежных средств «псевдо» инвесторов. Также были использованы схемы с майнингом криптовалюты.

6. В социальных сетях применяется и такая схема отъёма денежных средств: размещение постов с просьбой закупки средств защиты для врачей, пожертвования денег на оказание помощи заболевшим и подобное. Активация идёт через личный аккаунт пользователя для послед-

дующего получения конфиденциальной информации. Мошенники могут получить данные аккаунта, а с помощью установки специального программного обеспечения — доступ к паролю для программ интернет-банкинга пользователя.

По данным Генпрокуратуры [5], в России за первое полугодие 2020 г. на 76% выросло количество дел, связанных с интернетом и телефонным мошенничеством (рис. 3).



Рис. 3. Число случаев мошенничества (преступность по статьям ст. 159–159.6 УК РФ) в апреле-июне 2020 г. по сравнению с аналогичным периодом предыдущих лет

Fig. 3. The number of fraud cases during the self-isolation (crime under Articles 159–159.6 of the Criminal Code of the Russia) in April–June 2020 (compared to the same period of prior years)

Источник: [5].

Прокуратура за время самоизоляции зафиксировала 82,5 тыс. случаев мошенничества, из них 71% — посредством сети интернет и по телефону. Мошенничество с банковскими картами, за рассматриваемый период, возросло в два раза. По данным проведенного ВЦИОМ исследования «Телефонное мошенничество: масштабы и потери» от 7 июня 2021 г., 57% россиян за последние шесть месяцев получали звонки от телефонных мошенников (почти каждый пятый в виде СМС-сообщений). По количеству зафиксированных случаев лидирует Москва и Санкт-Петербург (70%), в меньшей мере это коснулось средних и малых городов. Самые часто используемые мошеннические схемы связаны с предложением банковских услуг (38%), банковские карты (27%), кредитование (8%), предложения перечислить денег (5%). Реже остальных используются «классические приёмы» о выигрыше призов и предложения медицинских услуг (по 3%). Почти каждый десятый (9%) кто подвергся «атаке» со стороны телефонных мошенников, понесли денежный ущерб, в том числе 6% — констатировали значительный ущерб⁷. Этому способствовало появление новых форм совершения незаконного изъятия денежных средств у граждан, а также сайт-клонов известных интернет-магазинов по продаже дорогой бытовой и компьютерной техники.

Популярные сайты с бесплатными объявлениями стали ещё одной площадкой для мошеннических схем. Размещая лоты с заведомо низкими ценами, злоумышленники разработали алгоритм переключения ссылки на «поддельную» (фишинговую) страницу курьерской доставки для перевода денег за товар и доставку. В период самоизоляции и массового перехода на удалённую работу произошел рост числа DDoS-атак на 15%. Возросло число утечек конфиденциальной информации и/или информации, представляющей коммерческую тайну через сотрудников компаний,

что связано прежде всего со сложностями контроля службами безопасности персонала, работающего на «удалёнке» [5].

Согласно исследованиям специалистов Банка России, в последнее время фиксируется значительный рост активности нелегальных форекс-дилеров, деятельность и услуги которых связаны с ограничительными мерами по борьбе с пандемией. Как правило, это иностранные интернет-площадки и компании. Потребители, которые размещают у них свои денежные средства, почти всегда теряют их. Банк России за I квартал 2020 г. выявил 369 нелегальных организаций, предлагающих услуги на финансовом рынке: финансовые пирамиды (37), «чёрные» кредиторы (254), нелегальные форекс-дилеры (53). Как и в предыдущие периоды произошло увеличение количества сайтов и платформ, которые связаны с криптовалютами, предлагающих заработок на данном рынке⁸.

Эксперты Лаборатории Касперского в апреле 2020 г. выявили 58 страниц, которые имитировали работу (мимикрировали) под известную площадку «Авито», в июле таких было уже 201. Общее число подделок под указанную интернет-площадку за семь месяцев 2020 г. превысило 500. Выросло число «подозрительных» ресурсов, которые не только обещают социальные выплаты в связи пандемией, но предлагают, например, пройти опрос за денежное вознаграждение. Далее схема аналогична большинству подобных ресурсов — это возможность получения обещанного гонорара только после перевода «закрепительного платежа» или «комиссии», а далее деньги уходят на счета злоумышленников. Растёт активность звонков «от службы безопасности банков» клиентам крупных банков, по классической схеме совершённых операциях, транзакциях для получения конфиденциальной информации пользователя для несанкционированного доступа к банковской карте с целью похищения денежных средств [5].

⁷ Телефонное мошенничество: масштабы и потери // ВЦИОМ: [сайт]. — URL: <https://wciom.ru/analytical-reviews/analiticheskiy-obzor/telefonnoe-moshennichestvo-masshtaby-i-poteri> (дата обращения: 24.11.2021).

⁸ Финансовые мошенники используют пандемию и неопределённость на рынках для обмана граждан // Банк России: [сайт]. — URL: <https://cbr.ru/press/event/?id=6710> (дата обращения: 24.11.2021).

Таким образом, в настоящее время практически все формы финансового мошенничества в той или иной степени связаны с информационно-коммуникационными технологиями (ИКТ). Новые технологии используются для получения необходимой информации, для распространения «вредоносного контента», как средство платежа, махинации с пластиковыми картами и так далее. По приведённым результатам исследования видно, что данная проблема становится ещё более актуальной в период пандемии. Большинство россиян имеют смутные представления о кибер- и финансовой безопасности.

В 2019 г. сотрудниками Лаборатории исследования поведенческой экономики ИСЭПН ФНИСЦ РАН было проведено исследование по вопросам адаптации социума к смене технологических укладов и внедрения новых ИКТ, изменения потребительской парадигмы и появления новых методов мошенничества (в сети интернет и кибер-мошенничества). Задача данного исследования заключалась в необходимости изучения влияния новаций в современном цифровом мире на индивида — конечного потребителя, в том числе, с точки зрения потенциальных угроз финансового мошенничества с использованием новых технических средств и интернет-технологий⁹.

Было установлено, что 92,9% респондентов каждый день пользуются интернетом, 3,8% — раз в неделю, 0,6% — раз в месяц и лишь 3,7% — не используют его вообще. Меньше трети (29%) не покупают товары через интернет, так как не видят в этом необходимости; 71% — покупают. При

этом для 77% опрошенных важно иметь возможность «потрогать» товар, для 8% — эта возможность не первостепенна, а для 15% — не имеет значения.

При совершении покупки через интернет важным становится вариант оплаты товара. С точки зрения мошеннических угроз — это самый уязвимый момент в электронной коммерции. У тех респондентов, которые пользовались интернетом для приобретения товара и/или услуг, уточнили способы оплаты (рис. 4). Больше половины (55%) расплачиваются карточкой при совершении покупки; 16% — предпочитают оплату при получении товара, 8% — получают и оплачивают покупки на почте. Почти столько же респондентов предпочитают пользоваться банковским переводом (8%) или платежными системами (9%); 4% — расплачиваются электронными деньгами.

Далее выявлялись факторы столкновения опрошенных с финансовыми мошенниками. На вопрос «Вы сталкивались с финансовыми мошенниками?» почти половина опрошенных (48%) ответили утвердительно. Причём 12% — респондентов в результате потеряли денежные средства (рис. 5).

Многие из опрошенных не в полной мере представляли в чём именно могут состоять современные способы мошенничества. На вопрос «С какими видами мошенничества Вы встречались?» только треть (31%) смогла ответить «не сталкивался» (рис. 6). Чаще всего респонденты указывали «сообщения в соцсетях от незнакомцев с просьбой положить (перевести) денег» (50%). Далее — «предложения вложить деньги в финансовую пирамиду» (13%), «получить кредитную карту по почте» (12%) и «приходили домой мнимые «социальные работники» (или другие «служащие»)» (11%).

Современные коммуникационные технологии становятся всё более доступными широким слоям населения, а следовательно, большее количество мошеннических схем сегодня реализуются именно в мобильных устройствах. Только 29%

⁹ География исследования — юго-восток Московской области: 6 городов (Коломна — 23%; Луховицы — 21%; Егорьевск — 13%; Воскресенск — 13%; Зарайск — 8%; Озёры — 8%) и 11 населённых пунктов в сельской местности (14%). Общее количество опрошенных составило 2500 человек (47% — мужчины, 53% — женщины). 48% — молодые люди в возрасте 18–29 лет; 6% — 14–17 лет; 32% — 30–49 лет; 13% — 50–70 лет; 1% — старше 70 лет. Квоты задавались на основе пропорционального соответствия их данным Росстата по составу населения в каждом населённом пункте. Наряду с этим, при опросе соблюдалась пропорция относительно населения юго-востока Подмосковья по количеству населения в городе, полу и возрасту, что позволяло обеспечить необходимую репрезентативность.



Рис. 4. Какой способ оплаты вы предпочитаете в Интернете?,%

Fig. 4. Which payment method do you prefer online?,%

Источник: авторские исследования.

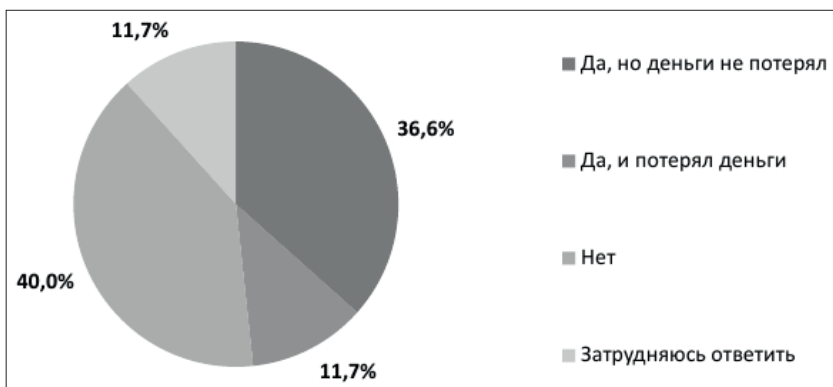


Рис. 5. Вы сталкивались с финансовыми мошенниками?,%

Fig. 5. Have you encountered financial fraudsters?,%

Источник: авторские исследования.



Рис. 6. С какими видами мошенничества Вы встречались?,%

Fig. 6. What types of fraud have you encountered?,%

Источник: авторские исследования.

опрошенных не сталкивались с «мобильным мошенничеством» по сотовому телефону (рис. 7).

Чаще всего — это СМС сообщение от незнакомцев с просьбой под любым предлогом «перевести деньги» (45%). Далее — различные варианты убеждения: «Вы вы-

играли автомобиль!» (27%); «Пожалуйста, верните деньги» (21%); «Ваш сын попал в аварию!» (17%); «Помогите ребёнку!» (13%); «Вы получили наследство!» (6%); «Пожалуйста, разрешите позвонить!» (5%).

Из всех респондентов лишь треть (31%) не сталкивались со случаями мошенни-



Рис. 7. С какими видами «мобильного мошенничества» (по телефону) Вы сталкивались?,%

Fig. 7. What types of "mobile fraud" (by phone) have you encountered?,%

Источник: авторские исследования.

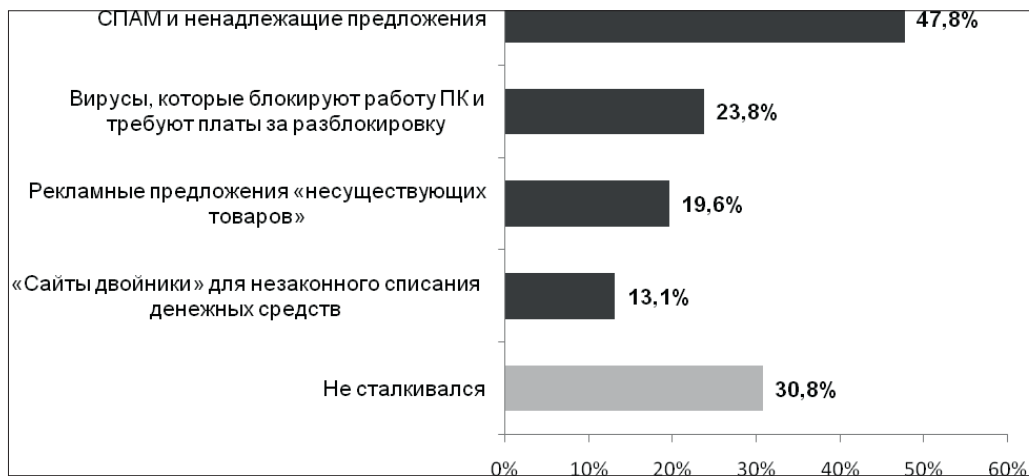


Рис. 8. С какими видами мошенничества в Интернете Вы сталкивались?,%

Fig. 8. What types of online fraud have you encountered?,%

Источник: авторские исследования.

чества в интернете (рис. 8). Почти половина опрошенных (48%) сталкиваются со спамом; 24% — стали жертвами «вирусов», которые блокируют работу компьютера и требуют платы за разблокировку; каждый пятый респондент (20%) получал рекламные предложения «несуществующих товаров»; 13% — попадал на «сайты двойники» для незаконного списания денежных средств; 43% — доля тех, кто из-за вирусов переустанавливал операционную систему или даже менял компьютер.

Большинство мошеннических схем сегодня связаны с платёжными системами.

Обычно это махинации с банковскими картами. Больше трети (37%) респондентов на вопрос «Считаете ли Вы, что банковские пластиковые карты сегодня надёжны и защищены?» дали отрицательный ответ; 45% — напротив, считают её надёжной и активно используют данное платёжное средство для оплаты товаров и услуг; 13% — не доверяют банковским картам в полной мере и снимают сразу все деньги, как только они на ней появляются. Менее 5% опрошенных не имеют пластиковую карту (рис. 9).

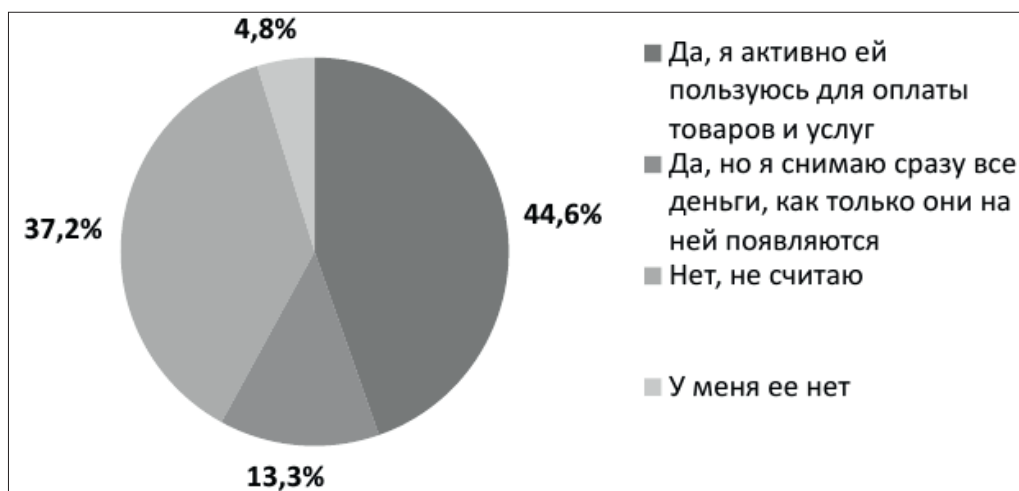


Рис. 9. Считаете ли Вы, что банковские пластиковые карты сегодня надёжны и защищены?,%

Fig. 9. Do you think that bank plastic cards are reliable and protected today?,%

Источник: авторские исследования.

Совершенствование и защита мобильных платёжных систем с каждым годом становится лучше. Однако 18% опрошенных респондентов сталкивались с ситуацией, когда со счёта (банковского, мобильного телефона, карточки и т.п.) незаконно списывали денежные средства. Как правило в этом обычно виноват сам пользователь, так как он сообщает злоумышленникам, которые позвонили под видом работника банка, pin-код карты или подтверждает запросы по СМС, а также открывает подозрительные ссылки и т.п.

Обычно именно безответственное поведение пользователя и/или его финансовая безграмотность, к сожалению, приводит к потере денежных средств.

* * *

Проведённое исследование позволило выявить современные тенденции потребления и связанные с ними возможные риски, прежде всего из-за финансового мошенничества, которое в последнее время (в том числе, в связи с эпидемиологиче-

скими ограничениями) приобретают новые формы. Проведённый авторами опрос показал, что почти половина респондентов сталкивались с финансовыми мошенниками в Сети; лишь треть не сталкивались. Почти половина опрошенных имели проблемы со спамом, 24% — стали жертвами «вирусов», каждый пятый получал рекламные предложения «несуществующих товаров»; 13% — попадал на «сайты двойники» для незаконного списания денеж-

ных средств. Как правило, в этом виноват и сам пользователь.

Полученные результаты опроса в малых городах юго-востока Подмоскovie могут быть использованы для профилактики совершения мошеннических действий, а также при проведении соответствующими структурами власти, комитетами и комиссиями занятий по обучению финансовой грамотности населения и других разъяснительных мероприятий.

Литература и Интернет-источники

1. **Шабунова, А. А.** Успешность современного человека: теоретико-методологические аспекты исследования / А. А. Шабунова, В. Г. Доброхлеб, Е. И. Медведева [и др.] // Экономические и социальные перемены: факты, тенденции, прогноз. — 2019. — Т. 12. — № 6. — С. 35–38. DOI: 10.15838/esc.2019.6.66.2.
2. **Ревина, С. Ю.** Электронная коммерция в России в условиях пандемических ограничений COVID-19 / С. Ю. Ревина, Д. А. Третьякова // Вопросы инновационной экономики. — 2021. — Т. 11. — № 4. — DOI: 10.18334/vines.11.4.113757.
3. **Шерemet, И. А.** Цифровая экономика и кибербезопасность её финансового сегмента / И. А. Шерemet // Труды Вольного экономического общества России. — 2018. — Т. 210. — № 2. — С. 23–35.
4. **Крошилин, С. В.** Финансовое мошенничество в современном обществе / С. В. Крошилин, Е. И. Медведева // Российский экономический конгресс «РЭК-2020». Том XVIII. Тематическая конференция «Банки и финансовые рынки» (сборник материалов) / составители С. А. Андрушин, А. М. Карминский. — Москва, 2020. — С. 83–87.
5. **Линделл, Д.** Число дел о мошенничестве рекордно выросло на фоне пандемии. Каким преступлениям поспособствовала самоизоляция / Д. Линделл, М. Алехина, А. Скрынникова, А. Балашова // РБК: [сайт]. — URL: <https://www.rbc.ru/society/31/08/2020/5f48ea169a79477e21e25d9d> (дата обращения: 24.11.2021).

Сведения об авторах:

Медведева Елена Ильинична, д.э.н., доцент, ведущий научный сотрудник, Институт социально-экономических проблем народонаселения Федерального научного исследовательского социологического центра Российской академии наук, Москва, Россия.

Контактная информация: e-mail: e_lenam@mail.ru; ORCID: 0000–0003–4200–1047; Researcher ID Web of Science: B-8964–2018; Scopus Author ID: 55925326400; PИНЦ Author ID: 381176.

Крошилин Сергей Викторович, к.э.н., старший научный сотрудник, Институт социально-экономических проблем народонаселения Федерального научного исследовательского социологического центра Российской академии наук; доцент кафедры математики, физики и медицинской информатики Рязанского государственного медицинского университета имени академика И. П. Павлова Министерства здравоохранения РФ, Рязань, Россия.

Контактная информация: e-mail: krosh_sergey@mail.ru; ORCID: 0000–0002–6070–1234; Researcher ID Web of Science: J-2184–2018; Scopus Author ID: 56292054500; PИНЦ Author ID: 664581.

DOI: 10.19181/population.2022.25.1.3

FINANCIAL FRAUD DURING THE COVID-19 PANDEMIC

Elena I. Medvedeva¹, Sergey V. Kroshilin^{1,2*}

¹*Institute of Socio-Economic Studies of Population of the Federal Center of Theoretical and Applied Sociology of the Russian Academy of Sciences (32 Nakhimovsky prospect, Moscow, Russian Federation, 117218)*

²*Pavlov Ryazan State Medical University (9 Vysokovolt'naya str., Ryazan, Russian Federation, 390026)*

*E-mail: krosh_servey@mail.ru

For citation:

Medvedeva E.I., Kroshilin S.V. Financial fraud during the COVID-19 pandemic. *Narodonaselenie [Population]*. 2022. Vol. 25. No. 1. P. 29-42. DOI: 10.19181/population.2022.25.1.3. (in Russ.)

Abstract. *The purpose of this study was to study new ways of financial fraud faced by Russian society during the pandemic. The object of the study is the Russian society, the subject is financial fraud schemes that became possible due to restrictive measures and the rapid development of online commerce during the pandemic. Modern society is facing various challenges, which are caused not only by progressive development technologies, innovations, changing technological patterns, rapid development and widespread introduction of information (digital) technologies, but also by factor whose appearance was difficult to predict—the Coronavirus pandemic. It has only been two years since the whole world has been living in the pandemic, but during this time the behavioral attitudes of society have undergone significant changes: from the “self-isolation regime” and the mandatory “wearing” of masks—to working “remotely” and the mandatory presentation of QR codes. Recent changes largely predetermined the rapid development of information and communication technologies, which affected real communication and the possibility of changing online behavior: shopping, getting certificates and documents, working remotely—50 to 80% of employees in various fields had to work at home. Going online entailed not only increased demand for communication services, development of Internet commerce, Internet banking (at the beginning of the pandemic, a mortgage purchase of housing was carried out completely online for the first time), but also contributed to creation of new types of financial fraud through communication technologies. The article uses the materials of the Federal Statistical Service, VTSIOM, the Bank of Russia, RBC, analytical materials of financial structures, analysts and the results of studies, including those by the author, conducted in the south-east of Moscow oblast. The results of the conducted research can be significant for prevention of fraudulent actions, as well as during classes on financial literacy of the population. The relevant authorities, committees and commissions can use these materials to conduct explanatory activities for the population.*

Keywords: *socio-economic problems, society, pandemic, coronavirus, financial fraud, e-commerce, information technology.*

References and Internet sources

1. Shabunova A. A., Dobrokhleb V. G., Medvedeva E. I., Kroshilin S. V., Sukhotska L., Shukhatovich V. R., Leonidova G. V., Molchanova E. V. Uspeshnost' sovremennogo cheloveka: teoretiko-metodologicheskiye aspekty issledovaniya [The success of modern man: theoretical and methodological aspects of research]. *Ekonomicheskiye i sotsial'nyye peremeny: fakty, tendentsii, prognoz [Economic and Social Changes: Facts, Trends, Forecast]*. 2019. Vol. 12. No. 6. P. 35–38. DOI: 10.15838/esc.2019.6.66.2. (in Russ.)
2. Revinova S. Yu., Tretyakova D. A. Elektronnaya kommertsiya v Rossii v usloviyakh pandemicheskikh ogranicheniy COVID-19 [E-commerce in Russia under the conditions of the COVID-19 pandemic restrictions]. *Voprosy innovatsionnoy ekonomiki [Issues of Innovative Economy]*. 2021. Vol. 11. No. 4. DOI: 10.18334/vinec.11.4.113757. (in Russ.)
3. Sheremet I. A. Tsifrovaya ekonomika i kiberbezopasnost' yeyo finansovogo segmenta [Digital economy and cybersecurity of its financial segment]. *Trudy Vol'nogo ekonomicheskogo obshchestva Rossii [Proceedings of the Free Economic Society of Russia]*. 2018. Vol. 210. No. 2. P. 23–35. (in Russ.)
4. Kroshilin S. V., Medvedeva E. I. Finansovoye moshennichestvo v sovremennom obshchestve [Financial fraud in modern society]. *Rossiyskiy ekonomicheskiy kongress «REK-2020». Tom XVIII. Tematicheskaya konferentsiya «Banki i finansovyye rynki» [Russian Economic Congress “REC-2020”. Volume XVIII. Thematic conference “Banks and Financial Markets”]*. Compiled by C. A. Andryushin, A. M. Karminsky. Moscow. 2020. P. 83–87 (in Russ.)
5. Lindell D., Alekhina M., Skrynnikova A., Balashova A. Chislo del o moshennichestve rekordno vyroslo na fone pandemii Kakim prestupleniyam posposobstvovala samoizolyatsiya [The number of fraud cases has grown record-breaking against the background of the pandemic. What crimes the self-isolation contributed to]. Available on: <https://www.rbc.ru/society/31/08/2020/5f48ea169a79477e21e25d9d> (Accessed 24 November 2021). (in Russ.)

Information about the authors:

Medvedeva Elena Ilinichna, Doctor of Economics, Associate Professor, Leading Researcher, Institute of Socio-Economic Problems of Population of the Federal Research Center of the Russian Academy of Sciences, Moscow, Russian Federation.

Contact information: e-mail: e_lenam@mail.ru; ORCID: 0000-0003-4200-1047; Researcher ID Web of Science: B-8964-2018; Scopus Author ID: 55925326400; Elibrary Author ID: 381176.

Kroshilin Sergey Viktorovich, Candidate of Technical Sciences, Associate Professor, Senior Researcher, Institute of Socio-Economic Problems of Population of the Russian Academy of Sciences; Associate Professor, Pavlov Ryazan State Medical University, Ryazan, Russian Federation.

Contact information: e-mail: krosh_sergey@mail.ru; ORCID: 0000-0002-6070-1234; Researcher ID Web of Science: J-2184-2018; Scopus Author ID: 56292054500; Elibrary Author ID: 664581.

Статья поступила в редакцию 03.12.2021, одобрена 28.02.2022, опубликована 30.03.2022.