

Формы финансового мошенничества в современном мире

УДК 316.42

DOI 10.26425/2658-347X-2025-8-2-55-64

Получено 09.04.2025

Доработано после рецензирования 01.07.2025

Принято 02.07.2025

Рахмеева Ирина Игоревна

Д-р экон. наук, зав. каф. экономической теории
и прикладной социологии

ORCID: 0000-0003-1431-7976

E-mail: rahmееva_ii@usue.ru

Уральский государственный экономический университет,
г. Екатеринбург, Россия

Попкова Светлана Викторовна

Студент

ORCID: 0009-0009-6994-2243

E-mail: popkova2016@bk.ru

Уральский государственный экономический университет,
г. Екатеринбург, Россия

АННОТАЦИЯ

Вследствие высокоразвитых современных информационных систем и технологий участились случаи мошенничества и появляются новые схемы обмана. Целью исследования является описание феномена финансового мошенничества в современном цифровом мире и поведения граждан, подвергающихся попыткам мошеннического обмана, для последующей разработки рекомендаций по борьбе с ним. Основным методом исследования выступал социологический опрос. Базой выступили слушатели экономического университета как социальная группа, отличающаяся более высоким уровнем финансовой и цифровой грамотности. По итогам опроса сделан вывод о том, что телефонные звонки являются наиболее распространенной формой мошенничества. Финансово грамотное население критически относится к звонкам с незнакомых номеров и информации, которую

сообщает оппонент. С другой стороны, уверенность в том, что грамотный человек не станет жертвой мошенников, снижает потребность в знаниях о действиях после хищения средств. Сделаны рекомендации, что гражданам следует внимательнее и критичнее относиться к подозрительной информации и призывам совершить какие-либо действия в интернет пространстве или по телефону; со стороны государства необходимо организовать информирование граждан о формах мошенничества, обеспечить большую выявляемость преступлений и защиту активов россиян и организаций; в свою очередь, фирмам следует повышать безопасность своих информационных порталов, информировать клиентов о возможных действиях мошенников и методах защиты их персональных данных.

Ключевые слова

Финансовое мошенничество, социология мошенничества, формы мошенничества, киберпреступность, цифровое мошенничество, мошенничество в цифровой среде, финансовая грамотность, цифровые компетенции, информационное пространство

Благодарности. Статья подготовлена в рамках научно-исследовательской работы «Региональная идентичность финансовой культуры населения, развитие навыков принятия финансово грамотных решений населением муниципальных образований Свердловской области» 2024 г., регистрационный номер 124082100046-0. Отчет в открытом доступе не публикуется.

Для цитирования

Рахмеева И.И., Попкова С.В. Формы финансового мошенничества в современном мире // Цифровая социология. 2025. Т. 8. № 2. С. 55–64.

© Рахмеева И.И., Попкова С.В., 2025.

Статья доступна по лицензии Creative Commons "Attribution" («Атрибуция») 4.0. всемирная
(<http://creativecommons.org/licenses/by/4.0/>).



Forms of financial fraud in the modern world

Received 09.04.2025

Revised 01.07.2025

Accepted 02.07.2025

Irina I. Rakhmееva

Dr. Sci. (Econ.), Head of the Economic Theory and Applied Sociology Department

ORCID: 0000-0003-1431-7976

E-mail: rahmееva_ii@usue.ru

Ural State University of Economics, Yekaterinburg, Russia

Svetlana V. Popkova

Student

ORCID: 0009-0009-6994-2243

E-mail: popkova2016@bk.ru

Ural State University of Economics, Yekaterinburg, Russia

ABSTRACT

As a result of highly developed modern information systems and technologies, cases of fraud have become more frequent and new schemes of fraud appear. The purpose of this study is to describe the phenomenon of financial fraud in the modern digital world and behaviour of citizens who are subjected to fraudulent deception attempts for the subsequent development of recommendations to combat it. The main research method is a sociological survey. The base is made of students from the economic university as a social group with a higher level of financial and digital literacy. The survey concluded that phone calls are the most common form of fraud. Financially literate people are critical of calls from unfamiliar numbers and

information that the opponent reports. On the other hand, the confidence that a competent person will not become a victim of fraud reduces the need for knowledge about actions after the theft of funds. Recommendations are made that citizens should be more attentive and critical of suspicious information and calls to perform any actions in the Internet space or by phone; the state should inform citizens about forms of fraud, ensure greater detection of crimes and protection of assets of the Russians and organisations; in turn, firms should intensively protect their information portals, inform customers about possible actions of fraudsters and methods for protecting their personal data.

Keywords

Financial fraud, sociology of fraud, forms of fraud, cybercrime, digital fraud, fraud in digital environment, financial literacy, digital competencies, information space

Acknowledgements. The article has been prepared within the framework of the research “Regional identity of the financial culture of the population, development of financially sound decision-making skills by the population of municipalities of the Sverdlovsk region”, 2024, the registration number is 124082100046-0. The report has not been published in the public domain.

For citation

Rakhmееva I.I., Popkova S.V. (2025) Forms of financial fraud in the modern world. *Digital sociology*. Vol. 8, no 2, pp. 55–64. DOI: 10.26425/2658-347X-2025-8-2-55-64



ВВЕДЕНИЕ / INTRODUCTION

Современная жизнь сосредоточена вокруг цифровых технологий. Благодаря научно-техническому прогрессу существование человека стало легче за счет новых, постоянно появляющихся цифровых систем, роботов, упрощенной, многообразной и очень удобной платежной системы. Несмотря на все преимущества такого удобства и мобильности, есть и серьезные недостатки. Главной проблемой высокоразвитых технологий в современном мире является постоянное усовершенствование новых схем мошенничества. Последние два-три года тема мошенничества особо актуальна, так как преступники ежедневно разрабатывают новые схемы обмана, на которые попадают не только пожилые люди и люди с невысокой финансовой грамотностью, но и высокообразованное население. Несмотря на большие усилия со стороны государства и банковских структур по мониторингу финансовых операций и предотвращению незаконных действий [Близкий, Будаева, Долгушкина, Гулуа, 2023], особо остро стоит проблема выявления мошенников и возмещения понесенного ущерба. Для разработки эффективных мер по снижению как уровня мошенничества в финансовой сфере, так и последствий действий мошенников важно учитывать не только технические способы осуществления правонарушений, но и поведенческие реакции отдельных категорий населения на разные способы воздействия.

Целью исследования является описание феномена финансового мошенничества в современном цифровом мире и поведения граждан, подвергающихся попыткам мошеннического обмана, для последующей разработки рекомендаций по борьбе с ним на основе полученных результатов социологического опроса. Задачи работы включали выявление современных форм мошенничества, частоты столкновения с ними, поведения респондентов в таких ситуациях.

ОБЗОР СОВРЕМЕННЫХ ИССЛЕДОВАНИЙ / REVIEW OF CURRENT RESEARCH

Вопросы финансового мошенничества исследуются представителями разных наук. Мошенничество в современном мире – это распространенное и постоянно эволюционирующее явление, адаптирующееся к технологическому прогрессу и меняющимся социальным условиям. Его масштабы огромны, они наносят значительный экономический и социальный ущерб. Если экономистов интересуют вопросы направлений и финансовых

последствий такого мошенничества, а юристов – организации ответственности за них, то социологи уделяют свое внимание социальному поведению злоумышленников и жертв. Наша работа сосредоточена на гражданах, подвергавшихся попыткам финансового мошенничества в свой адрес, поэтому рассмотрим более подробно некоторые результаты социологических исследований этой проблематики последних лет.

В целом научные труды по обозначенной проблеме можно разделить на несколько групп: исследование подверженности населения разным формам мошенничества (А.Ю. Сергеев, О.В. Широкова, Л.А. Бураева), влияние финансовой грамотности или цифровых компетенций (П.Ш. Шихгафизов, Е.В. Конищева, С.А. Котляров, М.В. Клейменов), поколенческих факторов на поведение жертв злоумышленников (Т.А. Аймалетдинов, М.В. Цимбал, В.В. Лысенко). Представленные авторы раскрывают тему в областях корпоративного мошенничества, киберпреступности, телефонного мошенничества, мошенничества на рынках и т.д.

Одной из главных проблем общества в современном мире является финансовая безграмотность. «Финансовая грамотность без понимания сути развития цифрового общества не дает возможности эффективно ставить и решать многие задачи» [Сергеев, Широкова, 2023, с. 61]. Стоит отметить, что знание осуществления финансовых операций и понимание экономических процессов дают человеку представление о реальном устройстве мира финансовой и банковской систем. Поэтому финансово грамотные люди с большей вероятностью могут распознать обман и знают, как предотвратить преступные действия оппонента.

Мошенничеством называется хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием [Клейменов, 2023]. В современном мире формы финансового мошенничества становятся все более разнообразными и сложными благодаря развитию технологий и глобализации финансовых рынков. Вопрос его популяризации в современном мире интересует каждого добросовестного гражданина, столкнувшегося хоть раз с противоправными действиями хищения личной информации или денежных средств. В своих исследованиях А.Ж. Койчиев подробно рассматривает черты, свойственные преступнику, осуществляющему кражу личной информации и денежных средств путем обмана через интернет. Исследования автора наводят на мысль о том, что для осуществления мошеннических действий в интернете злоумышленник должен обладать глубокими специальными знаниями

информационных и программных систем, поэтому чаще всего на такого рода преступления идут мужчины молодого возраста, имеющие высшее образование, семью, постоянное место работы и стабильный доход [Койчиев, 2021]. Также автор отмечает, что, несмотря на образованность, личность преступника отличается от добропорядочного гражданина системой ценностей, привитой ему обществом [Койчиев, 2020].

По данным телекоммуникационного ресурса ТАСС, преступления с использованием информационно-телекоммуникационных технологий в 2024 г. достигли рекордного максимума от общего числа преступлений с 2020 г., а именно 40 % от общего числа зарегистрированных в Российской Федерации (далее – РФ)¹. За 12 месяцев 2024 г. в стране было зарегистрировано 765,4 тыс. киберпреступлений, что на 13,1 % больше, чем за аналогичный период 2023 г. По данным Министерства внутренних дел (далее – МВД), в 2024 г. четыре преступления из 5 (84,8 %) были совершены с использованием интернета. Всего зарегистрировано 649,1 тыс. таких преступлений. Это на 23 % больше, чем годом ранее. Также в прошлом году выросло число киберпреступлений, совершенных с использованием средств мобильной связи. Если в 2023 г. их было зарегистрировано почти 303 тыс., то в 2024 г. это число увеличилось на 14,3 % и составило 346 тыс. При этом глава МВД РФ В.А. Колокольцев указывает, что «пострадавшими от незаконных действий в цифровой сфере становятся физические и юридические лица, в том числе государственные структуры. Киберпреступления наносят существенный вред экономике и имущественным правам граждан. МВД рекомендует прекращать разговор по телефону, если собеседник предлагает снять деньги и передать их для внесения на безопасный счет, поскольку так ведут себя только мошенники»². Также сигналом мошенничества служит просьба сообщить код доступа, поступивший в СМС (англ. short message service – служба коротких сообщений), при этом не только для банка, но и для доступа к личному кабинету на Едином портале государственных услуг или других сервисах.

Злоумышленники осуществляют преступные действия не только в отношении физических лиц, также их злодеяниям могут подвергнуться и фирмы. Любые из них приводят к большим финансовым потерям, которые негативно сказываются на бюджете домохозяйств и порождают убытки

в организациях. Иногда случается так, что проворачивать мошеннические действия могут сотрудники компании, в которой они работают. «В среднем 1 из 1 000 сотрудников обманывает свою организацию, в результате чего от мошеннических действий в России пропадает ежегодно более 2 трлн руб» [Пономарчук, 2020, с. 163]. По этой причине многие работодатели очень ответственно относятся к предполагаемым сотрудникам организации при приеме на работу и интересуются их рекомендациями с предыдущих мест работы.

По мнению А.Ж. Койчиева, большинство мошеннических действий происходит через всемирную сеть – интернет. С автором нельзя не согласиться, так как действительно благодаря тому, что фирмы и физические лица обязаны часть персональной информации размещать на интернет-ресурсах, преступники могут легко взломать порталы и похитить личные данные организации и ее клиентов. Наряду с киберпреступностью очень распространено телефонное мошенничество, также мошенников можно встретить при покупке или аренде жилья и на многих других рынках. Поэтому правоохранительные органы рекомендуют критически относиться к объявлениям на рынках купли-продажи, изучать продавцов и покупателей товаров и имущества.

Возникновение различных чрезвычайных ситуаций и нестабильность в обществе способствуют активизации действий киберпреступников [Бураева, 2020]. Они используют сложившуюся ситуацию как новую схему своего обмана и хищения. В большинстве случаев мошенники представляются сотрудниками правоохранительных органов, органов государственной власти, здравоохранения и т.д. с просьбой перейти по отправленной ими ссылке или продиктовать полученный код. Социальное благополучие является одним из ключевых факторов, влияющих на развитие киберпреступности в обществе. Как отмечают П.Ш. Шихгафизов, Е.В. Конищева, С.А. Котляров, «социальное благополучие неразрывно связано с качеством жизни, позволяет оценить успешность усилий по его повышению» [Шихгафизов, Конищева, Котляров, 2023, с. 63]. Чем выше социальное благополучие, тем меньше у населения соблазна заниматься мошенничеством, так как человек, который имеет свободный доступ к медицинской помощи, чувствует себя в безопасности, может беспрепятственно перемещаться по местности, имеет доступ к культурным ценностям и достаточный объем средств на все жизненно необходимые блага, с меньшей вероятностью будет заниматься преступной деятельностью.

¹ Коньков С. В России в 2024 году IT-преступления достигли пика за последние пять лет». Режим доступа: <https://tass.ru/proisshestiya/22978955> (дата обращения: 07.04.2025).

² Там же.

Обзор научной литературы и публикаций правоохранительных органов позволил систематизировать основные формы мошенничества по сферам и технологиям (рис. 1), объединив их в группы.

Достаточно новыми видами мошенничества являются киберпреступления, основанные на технологических способах, например фишинг (поддельные электронные письма, сайты для доступа к конфиденциальной информации). С появлением новых электронных денег, получивших название «криптовалюта», пришло мошенничество с криптовалютой. Злоумышленники используют схемы Понци, фальшивых ICO (англ. initial coin offering – первичное размещение токенов) и других методов для обмана инвесторов в криптовалюту. Также успешно развиваются схемы мошенничества с внедрением вредоносного программного обеспечения (далее – ПО). Такие программы поражают устройства методом распространения вирусов и программ-вымогателей, которые блокируют доступ к компьютеру или данным и требуют выкуп за их разблокировку. Мошенничество в социальных сетях продолжает набирать свою популярность. Злоумышленники создают фальшивые профили, взламывают аккаунты и распространяют мошеннические предложения через социальные сети.

Традиционно сохраняется мошенничество на рынках недвижимости и финансов, где совершаются наиболее крупные сделки. Активно применяются способы мошенничества с использованием социальной инженерии, смещаясь

от живого контакта к телефонным средствам коммуникации (фишинг – телефонные звонки с целью выудить конфиденциальную информацию, такую как пароли, номера кредитных карт и банковские данные), а также к применению искусственного интеллекта (далее – ИИ). Преступники активно внедряют такие технологии, как SIM-свопинг (англ. subscriber identification module – модуль идентификации абонента) – перенос номера телефона жертвы на SIM-карту мошенника для получения доступа к банковским счетам и другой личной информации, скимминг – использование устройств для считывания данных с кредитных карт в банкоматах или POS-терминалах (англ. point of sale – точка продажи). Таким образом, технологии позволяют мошенникам легко и быстро похищать чужие данные и проводить финансовые махинации максимально незаметно для жертвы.

Анализ научных исследований по вопросам поведения жертв мошенников показывает, что их податливость обусловлена рядом следующих психологических и социальных факторов [Игнатьева, 2024; Зотина, 2023; Беркович, Матрешина, Павлова, 2024].

Первый фактор – недостаток знаний в финансовой сфере. Жертвы, не обладающие достаточными знаниями о современных методах мошенничества, о финансовых процессах и технологиях, не способны распознать мошеннические действия.

Второй фактор – доверчивость и наивность отдельных социальных групп, в первую очередь детей и людей пожилого возраста.

Мошенничество с использованием социальной инженерии	Инвестиционное мошенничество	Мошенничество в сфере недвижимости, страхования	Кибермошенничество
Претекстинг (ложные сценарии с целью убедить раскрыть личную информацию или перевести деньги). Вишинг (телефонные звонки с целью выманить конфиденциальную информацию). Уличное мошенничество. Подставные лица. Нетрадиционные услуги (магия и пр.)	Пирамидальные схемы (обещание высоких доходов от инвестиций, но выплаты за счет средств новых участников). Мошенничество с криптовалютами (несуществующие или мошеннические криптовалютные проекты)	Поддельные арендные объявления для получения предоплаты. Мошенничество с кредитами, ипотекой (получение по поддельным документам). Поддельные страховые полисы (несуществующие). Мошенничество со страховыми выплатами (ложные страховые иски)	Вредоносное ПО (вирусы и троянские программы для кражи финансовой информации). Мошенничество с онлайн-покупками (фальшивые интернет-магазины). Фишинг (поддельные электронные письма, сайты для доступа к конфиденциальной информации)

Составлено авторами по материалам исследования / Compiled by the authors on the materials of the study

Рис. 1. Систематизация форм финансового мошенничества

Fig. 1. Systematisation of forms of financial fraud

Эти же социальные группы, а также женскую часть населения и людей, находящихся в трудной жизненной ситуации, отличает подверженность третьему фактору – эмоциональной уязвимости.

Мошенники также стремятся найти социально изолированную жертву, не склонную обсуждать свои финансовые решения с другими или не имеющую возможность это сделать.

Интернет и цифровые технологии предоставляют мошенникам новые возможности для совершения преступлений. Интернет и криптовалюты позволяют злоумышленникам оставаться анонимными. Нередко личности такого рода мошенников установить не удастся из-за возможности маскировки IP-адреса (англ. internet protocol address – уникальный номер устройства) персонального устройства преступника и возможности скрыться в пространстве интернета. По мнению В.В. Лысенко, цифровизация играет большую роль в развитии информационных технологий, что, соответственно, способствует легкой доступности информации для злоумышленников [Лысенко, 2024]. Современные преступники могут действовать из любой точки мира. Также стоит отметить слабую сторону правового регулирования и правоохранительной деятельности касательно цифровой информации. В некоторых случаях правоохранительные органы не способны эффективно бороться с мошенниками. Такие условия позволяют мошенникам успешно осуществлять преступные действия и оказываться не причастными к совершению преступления. Борьба с мошенничеством – сложная задача, требующая комплексного подхода, включающего в себя как технологические, так и правовые и образовательные меры. Постоянная бдительность и осведомленность являются ключевыми элементами защиты от преступников.

МЕТОДЫ И БАЗА ИССЛЕДОВАНИЯ / METHODS AND RESEARCH BASE

Коллективом социологической лаборатории Уральского государственного экономического университета в июне 2024 г. был проведен социологический опрос жителей Свердловской области по теме финансового мошенничества в рамках научно-исследовательского проекта по изучению финансовой культуры и навыков принятия финансово грамотных решений (регистрационный номер научно-исследовательского и опытно-конструкторского проекта 124082100046-0).

Целевой аудиторией стали обучающиеся экономического университета (слушатели программ бакалавриата и магистратуры) как социальная

группа, отличающаяся более высоким уровнем (относительно среднего уровня) финансовой и цифровой грамотностью.

В опросе приняли участие 184 чел. – мужчины и женщины в возрасте от 18 до 45 лет. Большинство опрошенных были с неполным высшим образованием – 42 %, с полным высшим образованием – 24 %, со средним специальным – 18 %. 51 % опрошенных были бездетными, почти 17 % имели двух детей, 16 % – трех и более, у 15 % один ребенок в семье. Треть респондентов в данное время нигде не работает, 14 % заняты в сфере торговли, 12 % – в сфере образования, более 6 % – в промышленности, 6 % – в финансовом секторе. Учитывая специфику изучаемой социальной группы, отметим, что она характеризуется невысоким уровнем доходов: так, 25 % опрошенных получали месячный доход до 20 тыс. руб., 38 % – в диапазоне 31–65 тыс. руб., чуть более 20 % респондентов зарабатывали более 66 тыс. руб. в месяц. При этом 22 % опрошенных проходили специализированные курсы по повышению финансовой грамотности.

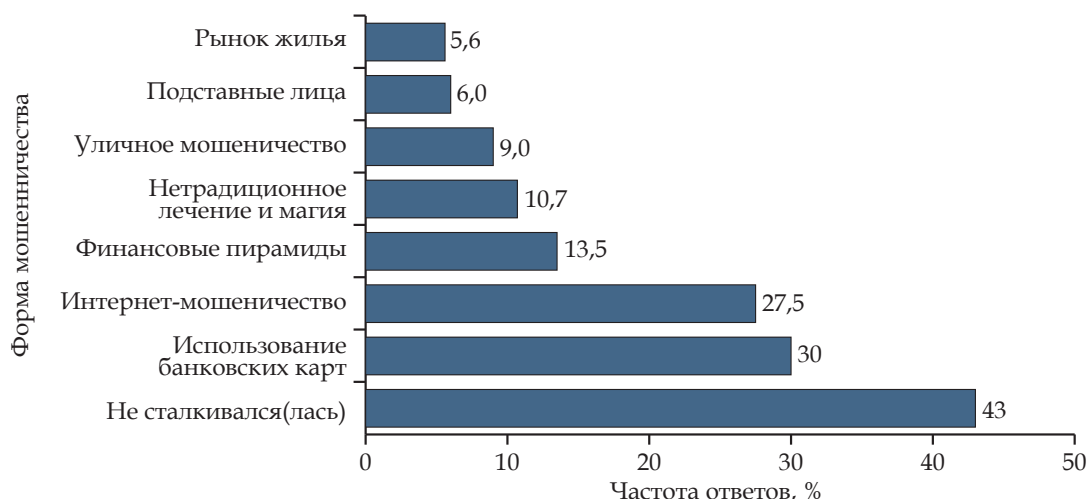
Анкетный вопрос был направлен на изучение форм мошенничества, с которыми сталкивались граждане, а также их поведения в ситуации наиболее распространенного вида мошенничества – по телефону.

РЕЗУЛЬТАТЫ СОЦИОЛОГИЧЕСКОГО ОПРОСА/ RESULTS OF THE SOCIOLOGICAL SURVEY

Одной из ключевых задач исследования было выявление спектра современных форм мошенничества. Результаты ответа на вопрос «С какими формами финансового мошенничества Вы сталкивались?», за исключением телефонных звонков, представлены на рис. 2.

Почти 43 % не сталкивались с финансовым мошенничеством или не помнят этого. Почти 30 % сталкивались с мошенничеством с использованием банковских карт; 27,5 % – с интернет-мошенничеством (лотерея, предложение работы и пр.); 13,5 % – с финансовыми пирамидами; 10,7 % – в сфере нетрадиционного лечения и магии, а также в сфере почтового и рекламного мошенничества; 9 % – с уличным мошенничеством; 6 % – с подставными лицами; 5,6 % – на рынке жилья.

Телефонные звонки остаются одной из самых распространенных форм мошенничества в современном мире. Так, 81 % респондентов сталкивались с ними, 13 % затруднились ответить на этот вопрос, будучи неуверенными, можно ли признать звонки в их адрес с неизвестных номеров мошенническими. Чуть больше трети



Составлено авторами по материалам исследования / Compiled by the authors on the materials of the study

Рис. 2. Распределение ответов на вопрос «С какими формами финансового мошенничества Вы сталкивались?»

Fig. 2. Distribution of answers to the question "What forms of financial fraud did you encounter?"

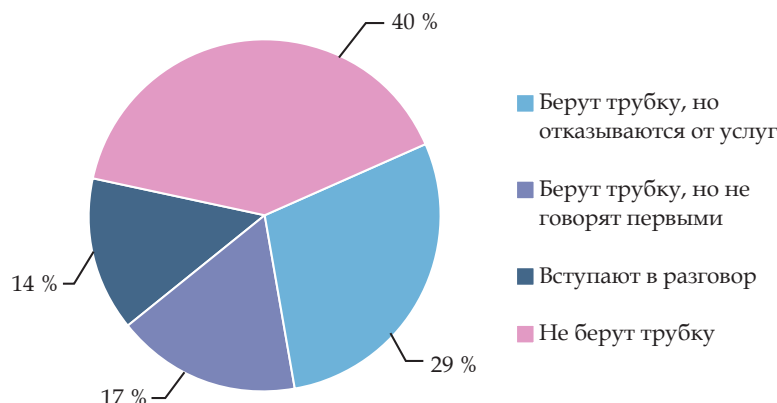
опрошенных сказали, что им звонили часто (один-два раза почти каждую неделю), 19,3 % – нечасто (один-два раза в месяц), 14,4 % – реже среднего (один-два звонка в полгода). Лишь 10,5 % респондентов звонили редко (пару раз в год).

Реакция на звонок от неизвестного номера представлена на рис. 3. В целом, в силу хорошей осведомленности населения о форме такого мошенничества и основных уловках, подавляющее большинство граждан знают главные правила поведения и способны обезопасить себя от последствий в виде финансовых потерь. Так, больше трети опрошенных не будут брать трубку с неизвестного номера, 29 % берут трубку, но отказываются от любого рода услуг, еще 17 % берут трубку, но не говорят первыми и 14 % берут трубку, но тщательно подбирают слова в разговоре.

Если все же респондент переведет деньги мошенникам, то 46 % опрошенных сообщат об этом

в сам банк или финансовую организацию (далее – ФО), из которой были переведены денежные средства (рис. 4). Треть опрошенных сообщит в полицию. К сожалению, 7,6 % респондентов не знают, куда обратиться, и еще 8,2 % затрудняются ответить. 3,8 % участников опроса вообще считают, что о факте мошенничества сообщит сама ФО, из которой были переведены деньги.

Таким образом, респонденты из числа слушателей экономического вуза осведомлены по вопросам предупреждения мошенничества лучше, чем по шагам, которые необходимо предпринять в случае реального совершения в отношении них противоправных действий с хищением средств. Возможно, такое поведение обусловлено их уверенностью, что они не смогут стать жертвами мошенников, хотя статистика демонстрирует обратное.



Составлено авторами по материалам исследования / Compiled by the authors on the materials of the study

Рис. 3. Поведение респондентов при поступлении звонка с неизвестного номера

Fig. 3. Behaviour of respondents when receiving a call from an unknown number



Составлено авторами по материалам исследования / Compiled by the authors on the materials of the study

Рис. 4. Поведение респондентов после перевода средств мошенникам

Fig. 4. Behaviour of respondents after transferring funds to fraudsters

ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ / DISCUSSION OF THE RESULTS

Число людей, сталкивающихся с мошенничеством в различных его проявлениях, значительно увеличивается ежегодно. Сравнивая результаты данного исследования с проведенными П.И. Ананчевой, И.А. Тюриным, К.К. Макаровой, Т.А. Аймалетдиновым, М.В. Цимбал опросами за 2021–2024 гг., в которых основной категорией граждан стали пожилые люди [Ананчева, Тюрин, Макарова, 2024; Аймалетдинов, Цимбал, 2024], отметим, что, в отличие от данной работы, сосредоточившей внимание на людях молодого возраста, можно сказать, что пенсионеры больше склонны подвергаться схемам мошенников, чем молодое поколение в силу большего доверия к окружающим и сопереживанию чужим проблемам, меньшей финансовой и цифровой грамотности.

Результаты исследования П.Ш. Шихгафизова, Е.В. Конищевой, С.А. Котлярова наводят на вывод о том, что уровень цифровой и финансовой грамотности влияет на качество современной жизни. Как показывает опыт, финансово грамотные люди с трудом поддаются схемам мошенников или вовсе не попадают на них, так как склонны подвергать сомнению информацию от незнакомых людей. Это подтверждает и данное исследование, в центре которого были потенциально более грамотные граждане, обучающиеся в экономическом университете, где они получают базовые знания по финансовым вопросам, а каждый пятый прошел курсы по финансовой грамотности.

На основе проведенного социального опроса на тему мошенничества можно заключить, что значительная часть опрошенных сталкивалась с различными формами мошенничества, но телефонные звонки на современном этапе являются

самой распространенной формой коммуникации злоумышленников с жертвами. Результаты проведенного нами исследования показали, что подавляющая часть респондентов сталкивалась со звонками злоумышленников, при этом многие из них подвергаются регулярным попыткам такого рода мошенничества. Меньше половины опрошенных не берут трубку, если звонят с неизвестного номера, другая же часть населения предпочитает вступать в разговор с незнакомыми, но быть осторожными. Вместе с тем схемы мошенников адаптируются под потенциальных жертв, они используют поддельные аккаунты знакомых и коллег жертвы, генерируют с помощью ИИ их голоса, звонят под видом представителей государственных служб, финансовых организаций или магазинов, куда недавно обращался гражданин.

ЗАКЛЮЧЕНИЕ / CONCLUSION

Подводя итоги, стоит сказать, что борьба с мошенничеством должна стать всеобщей общественной целью. Гражданам стоит внимательнее относиться к незнакомым звонкам, не выполнять никаких действий по просьбе оппонента, звонящего по телефону, проявлять осторожность в интернете, а также своевременно сообщать в правоохранительные органы о попытках мошенничества.

Государство занимается разработкой мер по защите населения от мошеннических действий. Развитие современных технологий позволило разработать новую услугу от приобретения нежелательных займов. Для того чтобы защитить свое финансовое положение от нежелательного кредита, оформленного мошенниками на имя жертвы, можно воспользоваться функцией, которую предлагает портал «Госуслуги», и установить

самозапрет на получение кредита. Благодаря такой операции злоумышленники не смогут оформить его на имя жертвы до тех пор, пока пользователь не отменит самозапрет самостоятельно путем личного обращения. В противном случае личность преступников будет раскрыта и злоумышленники понесут ответственность.

Для того чтобы побороть мошенническую деятельность, необходимо вводить определенный комплекс мер по борьбе с мошенничеством. Повышение финансовой грамотности населения и введение просветительской деятельности о мошеннических действиях помогут снизить вероятность того, что столкнувшийся с мошенничеством человек поддастся на провокацию, передаст персональные данные и иную критически значимую информацию. Правовое регулирование и усиление контроля за деятельностью в интернете, разработка правомерных и неправомерных действий и предусмотренные за неправомерные деяния в интернет-пространстве меры наказания смогут минимизировать киберпреступность.

Чтобы не попасться на мошеннические уловки, каждому необходимо помнить о методах защиты от схем злоумышленников. Существуют следующие рекомендации для граждан: относиться к незнакомой информации бдительно и скептически (не доверять той, что является слишком хорошей, чтобы быть правдой); не делиться личной информацией (не сообщать пароли, номера кредитных карт и другую конфиденциальную информацию по телефону, электронной почте или в социальных сетях); проверять информацию (убедиться, что имеете дело с законной организацией, прежде

чем предоставлять какие-либо данные или совершать платежи); использовать надежные пароли и антивирусное ПО; защищать свои устройства от вредоносного ПО; сообщать о мошенничестве в правоохранительные органы.

Фирмы тоже могут свести к минимуму вероятность похищения их конфиденциальной информации путем более надежной защиты своих информационных порталов и информированием клиентов с помощью разработанной инструкции с действиями в случае столкновения с мошенничеством. Также фирмам следует внимательно относиться к сотрудникам и следить за тем, чтобы в компании не появился мошенник, который бы действовал недобросовестно в отношении работодателя или клиентов компании.

Повышению финансовой грамотности населения могут поспособствовать курсы по обучению финансовой грамотности, на которых людям дают знания и навыки, необходимые для эффективного управления своими финансами. Они помогают принимать обоснованные финансовые решения, избегать долгов и достигать финансовых целей. В современном мире, где финансовые продукты и услуги становятся все более сложными, финансовая грамотность является необходимым навыком для каждого человека. Она помогает принимать взвешенные решения, достигать финансового благополучия и жить более комфортной жизнью. Необходимо помнить о том, что мошенничество постоянно эволюционирует, поэтому важно быть в курсе последних тенденций и методов, используемых преступниками, чтобы защитить себя и свои финансы.

СПИСОК ЛИТЕРАТУРЫ

- Аймалетдинов Т.А., Цимбал М.В. Восприятие современных технологий старшим поколением: сравнительный анализ. Цифровая социология. 2023;4(6):79–94. <https://doi.org/10.26425/2658-347X-2023-6-4-79-94>
- Ананченко П.И., Тюрин И.А., Макарова К.К. Роль цифровой социализации пожилых людей в защите от телефонного мошенничества. Цифровая социология. 2024;4(7):22–32. <https://doi.org/10.26425/2658-347X-2024-7-4-22-32>
- Беркович О.Е., Матрешина Е.Б., Павлова И.И. Социально-психологические причины и способы совершения мошенничества в современном обществе. Российский следователь. 2024;6:46–48. <https://doi.org/10.18572/1812-3783-2024-6-46-48>
- Бликий Р.С., Будаева Ю.Ж., Долгушкина В.А., Гулуа С.В. Технологии и тренды учета, отчетности и контроля в условиях развития цифровой среды государственного управления. Бухучет в здравоохранении. 2023;4:5–17. <https://doi.org/10.33920/med-17-2304-01>
- Бураева Л.А. О новых методах, используемых киберпреступниками, в условиях пандемии коронавируса. Проблемы экономики и юридической практики. 2020;2(16):308–310.
- Зотина Е.В. Антропология телефонного мошенничества с использованием претекстинга: криминологическое исследование. Мониторинг правоприменения. 2023;2(47):32–38. <https://doi.org/10.21681/2226-0692-2023-2-32-38>
- Игнатова Е.С. Манипуляция эмоциональной безопасностью кибермошенниками с применением технологий социальной инженерии: case-study. Вестник Пермского университета. Философия. Психология. Социология. 2024;3:374–390. <https://doi.org/10.17072/2078-7898/2024-3-374-390>

Клейменов М.В. Доверие как фактор развития финансовой грамотности населения в эпоху цифровой трансформации. В кн.: Финансовая грамотность: тренды, форматы, стратегические задачи развития: материалы I Международной научно-практической конференции, Екатеринбург, 2 ноября 2023 г. Курск: Университетская книга; 2023. С. 43–45.

Койчиев А.Ж. Детерминанты мошенничества в криминологии на примере интернет-сети. Вестник Кыргызского государственного университета имени И. Арабаева. 2020;3:200–203. <https://doi.org/10.33514/1694-7851-2020-3-200-203>

Койчиев А.Ж. Особенности аспекта мошенничества в юриспруденции. Известия Национальной академии наук Кыргызской Республики. 2021;S6:81–83.

Лысенко В.В. Цифровизация как интегральная тенденция современности. Цифровая компетенция и финансовая грамотность. В кн.: Финансовая грамотность: тренды, форматы, стратегические задачи развития: материалы II Международной научно-практической конференции, Екатеринбург, 15 октября 2024 г. Курск: Университетская книга; 2024. С. 74–76.

Пономарчук, А.В., Ахметова К.А. Корпоративное мошенничество: риски и влияние на экономическую безопасность бизнеса. Аллея науки. 2020;11(50(1):162–164.

Сергеев А.Ю., Широкова О.В. Мошенничество в цифровом обществе в условиях социальных изменений. Цифровая социология. 2023;1(6):59–71. <https://doi.org/10.26425/2658-347X-2023-6-1-59-71>

Шихгафизов П.Ш., Конищева Е.В., Котляров С.А. Влияние цифровой грамотности на субъективное благополучие молодого населения региона. Цифровая социология. 2023;4(6):61–66. <https://doi.org/10.26425/2658-347X-2023-6-4-61-66>

REFERENCES

Aimaletdinov T.A., Tsimbal M.V. Perception of modern technologies by the older generation: comparative analysis. Digital Sociology. 2023;4(6):79–94. (In Russian). <https://doi.org/10.26425/2658-347X-2023-6-4-79-94>

Anancheikova P.I., Tyurin I.A., Makarova K.K. Role of digital socialisation of the elderly in protecting against telephone fraud. Digital Sociology. 2024;4(7):22–32. (In Russian). <https://doi.org/10.26425/2658-347X-2024-7-4-22-32>

Berkovich O.E., Matreshina E.B., Pavlova I.I. Social and psychological causes and methods of fraud in modern society. Russian Investigator. 2024;6:46–48. (In Russian). <https://doi.org/10.18572/1812-3783-2024-6-46-48>

Blizkiy R.S., Budaeva Y.Zh., Dolgushkina V.A., Gulua S.V. Technologies and trends of accounting, reporting and control in the conditions of development of the digital environment of public administration. Accounting in Healthcare. 2023;4:5–17. (In Russian). <https://doi.org/10.33920/med-17-2304-01>

Buraeva L.A. On new methods used by cybercriminals in the context of the coronavirus pandemic. Economic problems and legal practice. 2020;2(16):308–310. (In Russian).

Ignatova E.S. Manipulation of emotional security by cybercriminals using social engineering technologies: a case study. Perm University Herald. Philosophy. Psychology. Sociology. 2024;3:374–390. (In Russian). <https://doi.org/10.17072/2078-7898/2024-3-374-390>

Klejmenov M.V. Trust as a factor in the development of financial literacy of the population in the era of digital transformation. In: Financial literacy: trends, formats, strategic development objectives: Proceedings of the I International Scientific and Practical Conference, Yekaterinburg, November 2, 2023. Kursk: University Book; 2023. Pp. 43–45. (In Russian).

Koichiev A.Zh. The determinants of criminology fraud on the example of the Internet network. Bulletin of Kyrgyz State University named after I. Arabaev. 2020;3:200–203. (In Russian). <https://doi.org/10.33514/1694-7851-2020-3-200-203>

Koichiev A.Zh. Features of the aspect of fraud in jurisprudence. Proceedings of the National Academy of Sciences of the Kyrgyz Republic. 2021;S6:81–83. (In Russian).

Lysenko V.V. Digitalisation as an integral trend of modernity. Digital competence and financial literacy. In: Financial literacy: trends, formats, strategic development objectives: Proceedings of the II International Scientific and Practical Conference, Yekaterinburg, October 15, 2024. Kursk: University Book; 2024. Pp. 74–76. (In Russian).

Ponomarchuk A.V., Akhmetova K.A. Corporate fraud: risks and impact on the economic security of business. Alley science. 2020;11(50(1):162–164. (In Russian).

Sergeyev A.Yu., Shirokova O.V. Fraud in a digital society in the context of social change. Digital Sociology. 2023;1(6):59–71. (In Russian). <https://doi.org/10.26425/2658-347X-2023-6-1-59-71>

Shikhgafizov P.Sh., Konischeva E.V., Kotlyarov S.A. Digital literacy impact on the subjective well-being of the region young population. Digital Sociology. 2023;4(6):61–66. (In Russian). <https://doi.org/10.26425/2658-347X-2023-6-4-61-66>

Zotina E.V. Anthropology of phone fraud using pretexting: a criminological study. Monitoring of Law Enforcement. 2023;2(47):32–38. (In Russian). <https://doi.org/10.21681/2226-0692-2023-2-32-38>