СОЦИАЛЬНЫЕ ПРОБЛЕМЫ СОВРЕМЕННОЙ РОССИИ

НАУЧНАЯ СТАТЬЯ

DOI: 10.21684/2587-8484-2023-7-2-67-97 **УДК** 316.4

Финансовое мошенничество в современном мире

Елена Павловна Данилова[1]
Екатерина Михайловна Портняга[2]

[1] кандидат социологических наук, доцент кафедры менеджмента и бизнеса, Тюменский государственный университет
e.p.danilova@utmn.ru; ORCID: 0000-0002-8254-2342

[2] лаборант-исследователь «Научно-исследовательского центра», Тюменский государственный университет
ekaterinaportnyaga@yandex.ru; ORCID: 0000-0002-0464-8838

Аннотация. С развитием цифровых транзакций и онлайн-банкинга существенно вырос риск финансового мошенничества. Технологии создали для мошенников новые возможности использования уязвимостей в финансовых системах и совершения преступлений. Понимание влияния технологий на финансовое мошенничество в разных странах имеет решающее значение для разработки эффективных стратегий предотвращения и борьбы с ним, а также оценки эффективности принимаемых мер.

В исследовании дается описание различных методов, используемых мошенниками для манипулирования цифровыми системами, рассматриваются уязвимости и пробелы в текущих мерах по борьбе с мошенничеством, анализируются данные и тенденции в области финансового мошенничества, выявляются закономерности в факторах, способствующих большей восприимчивости людей к мошенническим схемам.

Основная цель работы — оценить степень влияния технологий на финансовое мошенничество и сделать выводы о его влиянии на финансовые учреждения и частных лиц в различных географических точках, а также дать представление о влиянии технологий на финансовое мошенничество в разных странах и определить эффективные стратегии его предотвращения и выявления.

В заключение дается представление о решении текущих проблем финансового мошенничества и понимании важности использования передовых технологий для предотвращения мошеннических действий в будущем. Результаты исследования послужат ценной информацией для организаций, занимающихся управлением рисками и разработкой превентивной политики в непрерывно развивающейся технологической среде.

Ключевые слова: финансовое мошенничество, современные технологии, кибербезопасность, финансовая грамотность, кибермошенничество.

Цитирование: Данилова Е. П. Финансовое мошенничество в современном мире / Е. П. Данилова, Е. М. Портняга // Siberian Socium. 2023. Том 7. № 2 (24). С. 67-97.
DOI: 10.21684/2587-8484-2023-7-2-67-97

ВВЕДЕНИЕ

Финансовое мошенничество является постоянной угрозой в современном обществе, которая затрагивает отдельных людей, предприятия и правительства по всему миру. Мошенники продолжают изобретать новые изощренные методы обмана людей с целью получения финансовой выгоды. Эти мошеннические действия могут привести к значительным денежным потерям, эмоциональному расстройству и долгосрочному ущербу доверию между потребителями и организациями. Несмотря на различные меры предосторожности, принимаемые финансовыми учреждениями или правоохранительными органами, каждый день по-прежнему сообщается о бесчисленных случаях финансового мошенничества. Необходимо найти причины, почему подобные преступления совершаются во всем мире.

За последние несколько лет Россия столкнулась с несколькими громкими случаями финансового мошенничества, которые привели к значительным экономическим потерям. Например, в 2019 г. страна стала свидетелем масштабного скандала с хищениями, связанного с Национальной гвардией, которая потеряла более 120 млн долларов из-за мошеннической практики заключения контрактов. Кроме того, в 2018 г. российскому центральному банку пришлось отозвать лицензии у шестидесяти семи банков из-за их причастности к незаконной деятельности, такой как отмывание денег и уклонение от уплаты налогов.

Проблема финансового мошенничества представляет серьезную угрозу глобальной экономической стабильности и социальному благополучию, что требует тщательного изучения как академическим сообществом, так и профессионалами в сфере финансового сектора. Таким образом, предлагаемое научное исследование о влиянии технологий на финансовое мошенничество имеет важное значение, учитывая его потенциальную значимость для инвесторов, бизнес-менеджеров, политиков и регулирующих органов.

Поскольку мы вступили в цифровую эпоху, технологические достижения открыли новые возможности для совершения мошеннических действий. Новые тенденции проявляются все возрастающими темпами, что затрудняет выявление, предотвращение и решение проблем, связанных с цифровым финансовым мошенничеством. В предлагаемом исследовании будут изучены стратегии смягчения последствий, разработанные в разных странах, которые могли бы снизить риск финансовых махинаций, эволюционирующих с развитием технологий.

Для достижения цели исследования мы изучаем взаимосвязь между развитием технологий и финансовым мошенничеством при тщательном изучении распространенных мошеннических методов и выявляем возможные проблемы, связанные с этим развитием. Исследуя новые подходы к пресечению финансового мошенничества и анализируя их эффективность, исследование ставит акцент на разработке эффективных методов профилактики киберпреступности во всем мире.

Задачи исследования включают в себя следующее: изучить текущие тенденции и виды финансового мошенничества; проанализировать роль технологий в совершенствовании существующих практик или разработке новых методов финансового мошенничества; дать представление об успешных стратегиях борьбы с финансовым мошенничеством, реализованных в разных странах; предложить практические решения, которые уменьшат масштабы финансового мошенничества, совершаемого с помощью новых технологий.

Предметом исследования является влияние технологий на финансовое мошенничество, а также эффективные стратегии предотвращения и выявления финансового мошенничества.

Существующие исследования в этой области в основном посвящены анализу мошеннических практик и их последствий или методам предотвращения, основное внимание уделяется законам и нормативным актам отдельной страны или региона. Однако наше исследование направлено на изучение опыта многих стран и анализ потенциальных решений, связанных с финансовыми мошенничествами, которые могли бы помочь руководству нашей страны.

В исследовании выдвигается гипотеза о том, что, хотя технологии предоставляют возможности для инновационных стратегий смягчения последствий, но они одновременно играют определенную роль в содействии мошеннической деятельности. Анализируя успешную политику, проводимую в разных странах, это исследование позволит выявить лучшие практики, применяемые во всем мире, повысит уровень аналитических знаний в области финансового мошенничества, улучшив понимание эволюции моделей финансовых преступлений, а также позволит преодолеть разрыв в информационном обеспечении ученых из разных уголков мира. Кроме того, авторы статьи предлагают создать руководства для более эффективной борьбы с финансовыми преступлениями.

ОБЗОР ЛИТЕРАТУРЫ

Обзор российской и зарубежной научной литературы демонстрирует растущую озабоченность по поводу влияния технологий на финансовое мошенничество. Несмотря на наличие множества подходов к снижению этого риска, включая технологические инновации, искусственный интеллект и поведенческие вмешательства, многие проблемы все еще остаются нерешенными. Поэтому крайне важно провести дальнейшие исследования для определения более эффективных стратегий смягчения последствий, основанных на фактическом опыте борьбы с финансовым мошенничеством различных стран. Используя эти данные, государство и предприятия смогут определять наилучшие методы предотвращения мошеннических действий и защиты личной и финансовой информации.

Далее упомянутые ученые проводили исследование финансового мошенничества в России, особенно в отношении его влияния на банковский сектор. Например, Н. А. Чикишева отмечала, что в настоящее время характер мошенничества в России стал более изобретательным и приобрел интеллектуальный характер [13]. И. Я. Фойницкий ранее обратил внимание на то, что экономические факторы играют важную роль в распространении мошенничества. Он подчеркнул, что мошенничество является видом имущественного обмана, преступлением, которое развивается при значительном увеличении экономического оборота и имеет цивилизационное значение [12]. Исследование А. Е. Брусникина рассматривает проблему мошенничества на финансовом рынке, его основные виды и причины. Он предлагает несколько способов противодействия мошенничеству, включая усиление юридической ответственности, обучение и повышение квалификации персонала, а также разработку и внедрение новых технологий для обнаружения и предотвращения финансовых преступлений [3]. Ж. Е. Маронова рассматривает проблему мошенничества на финансовых рынках, особенности современных способов мошенничества и его экономическое влияние на общество [6]. Исследователь подчеркивает важность понимания мошенничества в финансовой сфере и необходимость постоянного совершенствования инструментов и методов его предупреждения. Л. А. Петрякова обсуждает проблему мошенничества в электронных платежных системах, особенности новых технологий в сфере электронных платежей и возможности противостоять преступлениям в данном направлении, рассматривает современные методы и формы мошенничества с использованием электронных средств платежа и анализирует возможные меры по их предотвращению [8]. В. А. Дадалко исследует поведение преступников, анализирует современные тенденции в области инноваций и практики предупреждения финансовых преступлений, рассматривает государственную политику в области борьбы с финансовыми преступлениями и предлагает практические рекомендации для предотвращения экономических преступлений на финансовом рынке, в том числе использование современных технологий и методов анализа больших данных [5]. С. В. Ревякин исследует особенности мошенничества, происходящего через современные электронные средства коммуникации, а также анализирует причины его возникновения. Он подчеркивает значимость данной проблемы для современного общества и необходимость разработки новых систем про-

филактики, которые бы обеспечивали безопасность пользователей современных электронных средств коммуникации [11]. В начале 1990-х гг. прошлого века отечественные ученые, такие как Ю. М. Батурин и А. М. Жодзишский, сформулировали концепцию компьютерной преступности. Они выделили два основных типа компьютерных преступлений, связанных с вмешательством в работу компьютера и с использованием его в качестве инструмента для совершения преступления [2]. Исследование О. Н. Головинова и А. В. Погорелова посвящено анализу киберпреступности в современном экономическом пространстве и тенденций его развития, особенно тех, которые связаны с постоянным развитием новых технологий и появлением новых способов совершения киберпреступлений [4]. Рассмотренные исследования посвящены проблемам кибербезопасности и модернизации финансовой системы, под угрозой которых находятся как отдельные люди, так и весь бизнес-сектор и государственные системы.

Поскольку финансовое мошенничество является глобальной проблемой, оно стало предметом исследования многих зарубежных ученых. Одной из популярных областей, представляющих интерес, является использование машинного обучения и искусственного интеллекта (ИИ) для выявления мошеннических действий. Например, К. Росси и О. Рибо пришли к выводу, что «возможности для развития инновационных видов мошенничества резко увеличились благодаря цифровизации». В докладе «Ориентация развития процессов анализа преступности в полицейских организациях, освещающих цифровую трансформацию механизмов мошенничества», авторы утверждают, что правительству необходимо разработать новые подходы к решению растущей проблемы онлайн-мошенничества, чтобы стать надежным партнером во взаимодействии с общественностью и другими заинтересованными профессиональными сторонами [50]. Исследование, проведенное М. В. Ахимом, В. Л. Вейдианом и Н.С. Борлеа (2021), исследует роль технологий в борьбе с экономическими и финансовыми преступлениями. Авторы утверждают, что достижения в области технологий как способствовали распространению этих преступлений, так и предоставили множество инструментов и методологий для их выявления и предотвращения. В целом исследование дает всесторонний обзор роли технологий в борьбе с экономическими и финансовыми преступлениями и предполагает, что технологии в сочетании с международным сотрудничеством могут играть значительную роль в выявлении и предотвращении этих преступлений [16]. Работа, авторами которой являются А. М. Босслер и Т. Бренблум (2019), представляет собой введение в новые направления исследований киберпреступности. Авторы утверждают, что киберпреступность быстро развивается и что характер и масштабы киберпреступности значительно изменились за последние годы, что требует новых подходов к пониманию этих тенденций и эффективного реагирования на них. Работа содержит всесторонний обзор текущего состояния исследований в области киберпреступности и освещает некоторые из продолжающихся дискуссий и проблем в этой области. Авторы предполагают, что существует необходимость междисциплинарного подхода, объединяющего знания из области компьютерных наук, криминологии, юриспруденции и социологии, для выработки более полного понимания киберпреступности [20]. Дж. Николлс, А. Куппа и Н. А. Ле-Хак (2016) исследуют потенциальную роль подходов глубокого обучения в борьбе с финансовой киберпреступностью. Авторы утверждают, что финансовая киберпреступность является серьезной и растущей проблемой, которая требует инновационных и изощренных решений. В исследовании делается вывод о том, глубокое обучение потенциально может произвести революцию в выявлении и предотвращении финансовых киберпреступлений, предоставляя более эффективные и точные методы анализа данных. Тем не менее, авторы также признают проблемы, связанные с внедрением подходов к глубокому обучению, включая проблемы конфиденциальности данных, высокие требования к вычислительной мощности и потенциал для враждебных атак [46]. В исследовании, авторами которого являются С. Рамадан, А. Путера и др. (2018), рассматривается влияние киберпреступности на технологическое и финансовое развитие

и утверждается, что киберпреступность является серьезной проблемой, которая затрагивает не только отдельных лиц и организации, но и оказывает более широкое воздействие на экономику и общество в целом [48].

Исследования демонстрируют, что достижения в области технологий способствовали распространению киберпреступной деятельности, но также предоставляют решения для выявления и предотвращения таких преступлений. Использование технологии блокчейна, искусственного интеллекта и машинного обучения, подходов к глубокому обучению и алгоритмов распределенного консенсуса являются примерами того, как технологии могут быть использованы для повышения безопасности, эффективности и отказоустойчивости кибернетических систем. Однако эти исследования также высвечивают проблемы и ограничения таких технологий, включая вопросы конфиденциальности данных, высокую стоимость внедрения и потенциальную возможность проведения кибератак.

В рамках социологических подходов к проблеме финансового мошенничества и определения его уровня, а также изучения экономического и финансового поведения можно выделить следующие направления зарубежных исследований: роль этической осведомленности и морального развития финансовых специалистов в предотвращении незаконного поведения в организациях: Дж. Берк, К. Киффер, Ф. Перес-Арсе, К. Льюис, Х. Ченг, К. Апичелла, Дж. Гарсия , Т. Стефан-Каталин, Т. Франкель, С. Харви, Дж. Керр, К. Ларс, С. Леа, Н. Шаховская, С. Федушко, Ю. Серов, Ф. Хайнцельманн, Дж. Бойл, М. Бенсон, М. Уитти; использование технологий для борьбы с финансовыми преступлениями: Р. Болтон, Д. Хэнд, К. Мейсон, Дж. Ли, Д. Шедель, Р. Титус, М. Бенсон; финансовое мошенничество и детектирование аномальных операций в банковской сфере: А. Хайнеманн, Дж. Джек, Т. Бенмарния, К. Швейцер-Пак, М. Зунзунеги, Ф. Беланд; финансовые мошенничества и коррупция в разных странах и регионах: Х. Коупс, Дж. Лангендерфер, Дж. Лэйн, Э. Беланже, М. Гоббо, А. Отеро; исследование финансовой преступности с использованием экспериментальных методов и психологических подходов: К. Керли, А. Дребер, Д. Айзенберг, Р. Заморе, Дж. К. Лум, Д. Вернер, С.Р. Мостафа, Дж. Нарумото, С. Ватанабе, Д. Ребович, К. Росси, О. Рибо, Н. Пикеро; финансовые мошенничества и киберпреступности: Г. Моттола, К. Пак, О. Дор, М. Бенсон, Б. Мытник, А. Ткачик. Перечисленные исследования о финансовых мошенничествах являются многообразными и охватывают различные аспекты данной проблемы. Они указывают на необходимость более внимательного и полного изучения этого явления, причин и последствий финансовых мошенничеств. Хотя исследования направлены на изучение разных аспектов финансовых мошенничеств, их общая цель заключается в выявлении эффективных мер борьбы с этим явлением. Многие исследования рассматривают вопросы этической осведомленности и морального развития финансовых специалистов, использование технологий и методов анализа данных для обнаружения финансовых мошенничеств, а также коррупции и киберпреступности.

Несмотря на то, что некоторые исследования фокусируются на одной конкретной области или стране, они имеют международное значение и их результаты могут использоваться во всех странах.

Общим выводом является то, что финансовые мошенничества являются значительной проблемой, которая требует единой стратегии и непрерывного изучения. Концепция полного предотвращения несовершенств в законодательстве, регулировании, профессиональном и моральном воспитании и этической осведомленности и технологических средствах защиты может снизить количество проявлений финансовых мошенничеств и ослабить их негативные последствия.

ОСНОВНАЯ ЧАСТЬ

Методы

При подготовке статьи авторами использовался метод контент-анализа научной зарубежной литературы и официальных сайтов финансовых учреждений. Были изучены и проанализированы 44 источника за период 1994-2023 гг.

Результаты и обсуждение

Финансовое мошенничество граждан, связанное с использованием технологий и уязвимостей в целях мошенничества и обмана для получения денежных переводов и личной информации, вызывает растущую озабоченность во всем мире.

Финансовое мошенничество — это вид обмана, который нацелен на отдельных лиц или организации с целью их финансовой эксплуатации. Оно может включать в себя, среди прочего, такие схемы, как фишинг, кража личных данных, мошенничество с инвестициями или поддельные призы в лотереях, и часто приводит к значительным финансовым потерям для вовлеченных жертв.

Виды финансового мошенничества, обычно используемые преступниками для эксплуатации граждан, эволюционировали со временем и технологическими достижениями. Телефонные звонки или сообщения с запросом личной информации — вот некоторые из распространенных способов, с помощью которых недобросовестные лица используют в своих интересах ничего не подозревающих людей. Некоторые из распространенных форм финансового мошенничества, нацеленного на граждан, включают:

- Фишинг. Это мошеннические электронные письма или текстовые сообщения, рассылаемые киберпреступниками, выдающими себя за законные учреждения. Они направлены на то, чтобы обманом заставить человека разгласить конфиденциальную информацию, такую как номера банковских счетов, пароли или номера социального страхования.
- Социальная инженерия. Этот тип мошенничества предполагает установление взаимопонимания или связи с человеком с помощью каналов коммуникации, таких как телефонные звонки, электронная почта или платформы обмена сообщениями. Цель состоит в том, чтобы заставить жертву доверять своему новому знакомому настолько, чтобы он мог поделиться важной информацией или участвовать в финансовых операциях.
- Скимминг / мошенничество с банкоматами. В рамках этой схемы преступники подключают к банкоматам небольшие устройства, известные как скиммеры, чтобы они могли незаконно собирать данные карт пользователей. После сбора преступник может использовать эти данные для таких действий, как онлайн-покупки, денежные переводы и т.д.
- Взлом. Кибератаки раскрывают конфиденциальную личную информацию граждан, включая имена пользователей, пароли и данные кредитных карт, подвергая их риску быть обманутыми.

По мере развития технологий растет и изощренность мошенничеств. Финансовым учреждениям приходится сотрудничать с директивными и правовыми органами в разработке практических мер, которые защищают общественность от угроз мошенников и одновременно способствуют формированию культуры ответственной финансовой практики. Только реализуя комплексные стратегии, ориентированные на образование, инициативы по повышению осведомленности и развивающиеся технологические решения, государство может добиться прогресса в защите финансовых систем от современных преступников.

Важно отметить, что жертвой финансового мошенничества может стать любой человек, независимо от его возраста, пола или социально-экономического положения. Хотя не существует определенной категории людей, которые более восприимчивы к подобным мошенничествам, некоторые группы, как правило, сталкиваются с более высокими рисками. Например, пожилые люди обычно становятся мишенью мошенников из-за их уязвимости и потенциального недостатка технологических знаний. Иммигранты или отдельные лица, не владеющие местным языком, также могут подвергаться более высокому риску, поскольку им трудно понимать юридические документы, связанные с финансами. Более того, домохозяйства с низким доходом часто сталкиваются с финансовыми трудностями и, следовательно, часто более уязвимы перед предложениями быстрой и легкой прибыли, предлагаемыми мошенниками.

Защита той части населения, которая подвергается финансовому мошенничеству, требует

принятия различных стратегий, направленных на полное предотвращение подобных инцидентов. Одним из жизненно важных методов является повышение осведомленности общественности посредством образовательных кампаний о распространенных типах мошенничества и методах их предотвращения, направленных конкретно на пожилых людей или другие демографические группы. Финансовые учреждения и регулирующие органы должны предоставлять четкие руководящие принципы и меры по защите финансовой информации клиентов, включая разработку протоколов для сообщения о любой подозрительной деятельности. Внедрение систем двухфакторной аутентификации и регулярная смена паролей могут усилить безопасность и отпугнуть хакеров.

Более того, сама технология может обеспечить потенциальные решения для борьбы с финансовым мошенничеством. Автоматизированный мониторинг транзакций, биометрическая аутентификация, искусственный интеллект (ИИ), алгоритмы машинного обучения и анализ больших данных позволяют выявлять нарушения в финансовой деятельности и точно идентифицировать потенциальные мошеннические транзакции. Чат-боты на базе искусственного интеллекта также могут помочь регулирующим органам в сборе информации о подозрительной деятельности или сообщениях о мошенничестве, тем самым повышая оперативность реагирования и экономя время.

Многие исследователи строили модели и опросы, пытаясь понять, как различные факторы объединяются и влияют на склонность становиться жертвами попыток финансового мошенничества.

Дж. Ли и Х. Соберон-Феррер предположили, что когнитивный дефицит и социальное взаимодействие влияют на тенденцию становиться жертвами мошенничества, поскольку оба связаны с биологическими, экономическими, социологическими и психологическими особенностями. Когнитивный дефицит относится к ограниченной способности некоторых людей обрабатывать информацию, что делает их более уязвимыми. На когнитивные способности влияет процесс старения, знания и опыт людей. С другой стороны, социальное взаимодействие относится к качеству социальных сетей и уровню социальной изоляции. Низкий уровень социального взаимодействия, будь то пожизненная социальная изоляция или контекстуальная (из-за негативных событий), делает людей более уязвимыми перед мошенниками. Причем психологическая изоляция играет в этом процессе более высокую роль, чем физическое одиночество [43].

С.И. Леа и др. (2009) сравнили потерпевших и не потерпевших относительно степени вероятности стать жертвой из-за неверных суждений и обнаружили, что склонность жертв к неверным суждениям выше среди жертв, чем среди не потерпевших. Авторы сделали вывод, что потерпевшие поддаются убеждению в целом, а не обязательно в отношении конкретного вида мошенничества, в которое попали потерпевшие. Они выявили различные факторы, связанные с неверным суждением в отношении финансового мошенничества, и разделили их на две группы. К первой группе относятся мотивационные факторы, такие как:

- мотивация базовых потребностей и желаний человека (страх, жадность, внутреннее влияние);
- поиск азарта в риске;
- отсутствие самоконтроля;
- низкая мотивация обработки информации;
- взаимность как стремление отплатить услугой за услугу;
- обязательства и последовательность: мошенник пользуется потребностью жертвы в установлении контакта и взаимодействии, а затем обращается к ней, чтобы вложить деньги.

Вторая группа включает следующие когнитивные факторы:

- позитивные иллюзии как склонность личности воспринимать себя в выгодном свете и оценивать свои способности;
- предварительные знания в конкретной области и самоуверенность в способности принимать правильные решения;
- низкие когнитивные способности (особенно у пожилых людей);

- информационное социальное влияние;
- использование норм поведения, таких как обращение к другим и вежливое поведение;
- склонность признавать авторитет [42].

Вопреки распространенному мнению, что поведение жертв иррационально, С. Харви и др. (2014) опросили 31 жертву инвестиционного мошенничества и обнаружили, что они действительно принимали рациональные решения. Благодаря качественным интервью с лицами, пострадавшими от финансовых преступлений, исследование дает представление о том, каким образом граждане становятся жертвами и как они начинают доверять мошенникам. В исследовании подчеркивается эмоциональное воздействие финансового мошенничества на жертв и необходимость повышения уровня образования и осведомленности об инвестиционных аферах. Жертвы показали, что они решили инвестировать в финансовые схемы исходя из сочетания финансовых, семейных и психологических обстоятельств на момент мошенничества:

1. Финансовые обстоятельства:

а) наличие финансовых ресурсов (даже изменение финансового положения);

б) восприятие систем и финансовых учреждений;

в) социальные и финансовые сети, включая их качество.

2. Семейные обстоятельства:

а) стремление быстро увеличить семейный доход;

б) потребность в долгосрочной финансовой безопасности для семьи.

3. Психологические обстоятельства (доверие, надежда, жадность и отчаяние) [35].

Уровень предварительных знаний в финансовой сфере играет важную роль в привлечении жертв мошенничества, даже если мнения относительно этой роли разделились. ААП (Американская ассоциация пенсионеров) (1999), Дж. Лангендерфер и Т. А. Шимп (2001) и Ё. Кадоя и др. (2021) обнаружили, что отсутствие предварительных знаний о мошенничестве или в области, связанной с конкретным мошенничеством (например, финансовым или инвестиционным), увеличивает вероятность стать жертвой мошенничества [14; 40, с. 763-783; 38]. Почти 75% жертв, опрошенных ААП (2007), имеют низкий уровень знаний о финансовых инвестициях [15]. Напротив, С. Леа и др. (2009) утверждают, что предварительное знание увеличивает шанс стать жертвой, потому что перед лицом такого знания жертва ведет себя менее осторожно. Во многих случаях жертвы инвестиционного мошенничества обладают предварительными знаниями в области финансовых инвестиций [42]. Д. Ребович и Дж. Лейн (2000) обнаружили, что жертвы инвестиционного мошенничества финансово более грамотны, чем население в целом [49].

Социально-демографическая динамика жертв финансовых махинаций включает основные характеристики по возрасту, полу, образованию, семейному и профессиональному положению. Было обнаружено, что только возраст и образование играют важную роль в прогнозировании тенденции стать жертвами личного мошенничества (Р. М. Титус и др.; Дж. Ван Вик и М. Л. Бейсон; К. Р. Керли и Х. Коупс) [53, с. 54-72; 54, с. 163-179; 39, с. 19-35]. Дж. Ли и О. Соберон-Феррер (1997) предположили, что возраст, образование и семейное положение оказывают значительное влияние на прогнозирование жертв, в то время как возраст оказывает наибольшее влияние [43, с. 70-89]. Однако некоторые ученые определили профили жертв с учетом упомянутых выше основных демографических характеристик, далее мы рассмотрим их подробнее (Д. П. Шадель, К. Б. Швейцер-Пак; М. В. Зунзунеги и др.) [52; 57, с. 313-319].

Р.М. Титус и др. (1995) предположили, что молодые люди чаще становятся жертвами из-за более низкого дохода и более высокого уровня восприимчивости к возможностям быстрого роста дохода, в то время как пожилые люди более склонны сообщать о мошенничестве, и по этой причине мошенники избегают их [53, с. 54-72]. Кроме того, риск для взрослых стать жертвой мошенничества в три раза ниже, чем для молодежи. Дж. Ван Вик и М.Л. Бейсон (1997) заявили, что молодые люди более склонны становиться жертвами финансовых махинаций, поскольку

мошенники считают, что молодые люди склонны больше рисковать [54, с. 163-179]. А. Шепфер и Н. Л. Пикеро (2009) подчеркнули склонность молодых людей идти на больший финансовый риск, что еще больше повышает их склонность становиться жертвами [51, с. 209-215]. Молодые люди, как правило, становятся жертвами предложений о возможностях бизнеса и работы на дому, мистицизма и сетевого мошенничества. С другой стороны, пожилое население обычно становится жертвой мошенничества в отношении высокорисковых инвестиций и поставщиков услуг, которые приходят на дом. М. Делиема и др. (2020) указали, что шансы стать жертвой инвестиционного мошенничества растут на 4% с каждым годом увеличения возраста [25, с. 904-914]. Д. Ребович и Дж. Лейн (2000) опросили 2100 человек, и демографические данные выборки были репрезентативными для населения США. В исследовании использовался структурированный опросный лист для сбора информации об опыте лиц, ставших жертвами преступлений «белых воротничков» (чиновники, служащие, управленцы, инженерно-технические работники и т. п.). Анкета была разработана для получения информации о типах преступлений, с которыми столкнулись жертвы, характеристиках правонарушителей, воздействии преступлений на жертв и их восприятии реакции системы уголовного правосудия на преступления «белых воротничков». Среди тех, кто сообщил, что стал жертвой, наиболее распространенными видами правонарушений были мошенничество с потребителями, мошенничество с телемаркетингом и финансовые пирамиды. 60% из них считали, что пожилые люди чаще всего становятся жертвами мошенничества [49].

В табл. 1 представлен сравнительный анализ исследований жертв финансового мошенничества по возрасту, распределенный по авторам [15].

Таблица 1. Исследования жертв финансового мошенничества по возрасту
Table 1. Research of financial fraud crime victims by age

Автор	Изучаемый период	Большинство жертв
М. Локанан (2014)	1984-2008	Пожилые люди
Дж. Ван Вик и М.Л. Бейсон (1997)	1989-1994	Молодые люди
Р.М. Титус и др. (1995)	1990-1991	Молодые люди
Дж. Ли и О. Соберон-Феррер (1997)	1993	Пожилые люди
И. Шихор и др. (1996)	1994	Пожилые люди
К.Р. Керли и Х. Коупс (2002)	1994	Молодые люди
ААП (Американская ассоциация пенсионеров) (1999)	1998	Пожилые люди
А. Шепфер и Н.Л. Пикеро (2009)	1999	Молодые люди
Дж. Э. Маскат и др. (2002)	2000	Молодые люди
Т. Паско и др. (2006)	2005	Молодые люди
ААП (Американская ассоциация пенсионеров) (2007)	2006	Пожилые люди
И.А. Болимос и Ким-Кванг Р. Чу (2017)	2008-2013	Пожилые люди
С. Харви и др. (2014)	2013	Пожилые люди
М. Батон и др. (2014)	2014	Пожилые люди
К. Сюй (2022)	2015	Пожилые люди
М.В. Зунзунеги и др. (2017)	2015-2016	Пожилые люди
М. Делиема и др. (2020)	2016	Пожилые люди
Ё. Кадоя и др. (2021)	2020	Пожилые люди
Ю.С.К. Ян и др. (2022)	2022	Пожилые люди

Что касается пола, мужчины, как правило, становятся жертвами иностранного мошенничества, сетевого мошенничества, высокорискованных инвестиций и инвестиций в землю, в то время как женщины уязвимы для сетевого мошенничества, продуктов для здоровья и похудения, которые обещают чудеса, мошенничества с мистицизмом и фальшивой карьеры, предложения по продвижению. Однако почти все ученые установили, что большинство жертв финансовых махинаций — мужчины (см. табл. 2) [28]. Дж. Ли и О. Соберон-Феррер (1997) обнаружили, что пожилые женщины более уязвимы для того, чтобы стать жертвами, чем пожилые мужчины, но для более молодых групп ситуация обратная [43, с. 70-89].

Таблица 2. Исследования жертв финансового мошенничества по полу
Table 2. Research of financial fraud crime victims by gender

Автор	Изучаемый период	Большинство жертв
М. Локанан (2014)	1984-2008	Мужчины
Дж. Ли и О. Соберон-Феррер (1997)	1993	Как мужчины, так и женщины
И. Шихор и др. (1996)	1994	Мужчины
Т. Паско и др. (2006)	2005	Мужчины
ААП (Американская ассоциация пенсионеров) (1999)	2006	Мужчины
Д.П. Шадель, К.Б. Швейцер-Пак (2007)	2006-2007	Мужчины
И.А. Болимос и Ким-Кванг Р. Чу (2017)	2008-2013	Мужчины
С. Харви и др. (2014)	2013	Мужчины
М. Батон и др. (2014)	2014	Мужчины
К. Сюй (2022)	2015	Мужчины
М.В. Зунзунеги и др. (2017)	2015-2016	Мужчины
М. Делиема и др. (2020)	2016	Мужчины
Д. Вуд и др. (2018)	2018	Мужчины
Европейская комиссия (2020)	2019	Мужчины
Ё. Кадоя и др. (2021)	2020	Мужчины
Ю.С.К. Ян и др. (2022)	2022	Мужчины

Как правило, образование рассматривается как фактор, влияющий на склонность становиться жертвой, поскольку люди используют навыки, полученные в ходе формального обучения, при принятии решений, включая финансовые [43, с. 70-89]. Дж. Берк и др. (2022) указали, что восприимчивость людей к становлению жертвами инвестиционного мошенничества может быть уменьшено с помощью образования, особенно образовательных онлайн-мероприятий [21, с. 250-266]. Исследование, проведенное Б.Л. Эльдадом, М. Ливиу-Джорджем и Т. Стефаном-Каталином (2022), направлено на выявление профилей жертв финансовых махинаций в развивающихся странах. Исследование основано на систематическом обзоре научных статей, отчетов и опросов, в которых обсуждается финансовое мошенничество в развивающихся странах. Авторы использовали подход тематического анализа для выявления ключевых тем и закономерностей, связанных с профилями жертв. Тем не менее литература неоднозначна в отношении уровня образования в профилировании жертв, и не было установлено четкой закономерности во времени, которое исследовалось авторами (см. табл. 3) [28]. С одной стороны, высокообразованные лица чаще

становятся жертвами мошенничества по ряду причин, даже если они умеют оценивать риски лучше, чем менее образованные люди. Одна из причин заключается в том, что они считают себя образованными и экспертами в своей области, и они применяют это суждение к тем областям, в которых они не очень подготовлены. Они считают, что защищены от мошенничества благодаря своему интеллекту. К. Р. Керли и Х. Коупс (2002) и А. Шепфер и Н. Л. Пикеро (2009) расширяют анализ, утверждая, что образование является переменной, тесно связанной с фактом сообщения о преступлениях, и предполагая, что люди с более высоким уровнем образования с большей вероятностью сообщат властям о мошенничестве [39, с. 29-35; 51, с. 209-215]. Х. Коупс и др. (2001) утверждают, что на решение сообщить о мошенничестве влияют такие факторы, как уровень образования, семейное положение, возраст и то, был ли преступник незнакомцем для жертвы [24, с. 343-363]. С другой стороны, некоторые ученые указывали, что люди с низким уровнем образования имеют более высокий риск стать жертвами финансового мошенничества. Дж. Ли и О. Соберон-Феррер (1997) обнаружили, что уровень уязвимости снижается по мере повышения уровня образования и дохода [43, с. 70-89].

Таблица 3. Исследования жертв финансового мошенничества по уровню образования
Table 3. Research of victims of financial fraud crime by level by education

Автор	Изучаемый период	Большинство жертв
Дж. Ван Вик и М.Л. Бейсон (1997)	1989-1994	Высокообразованные
Р.М. Титус и др. (1995)	1990-1991	Высокообразованные
Дж. Ли и О. Соберон-Феррер (1997)	1993	Менее образованные
И. Шихор и др. (1996)	1994	Высокообразованные
К.Р. Керли и Х. Коупс (2002)	1994	Менее образованные
ААП (Американская ассоциация пенсионеров) (1999)	1998	Менее образованные
Д.П. Шадель, К.Б. Швейцер-Пак (2007)	2006-2007	Высокообразованные
М.В. Зунзунеги и др. (2017)	2015-2016	Менее образованные
Д. Вуд и др. (2018)	2018	Менее образованные
Европейская комиссия (2020)	2019	Высокообразованные
Ю.С.К. Ян и др. (2022)	2022	Высокообразованные

Судя по исследованиям, которые проводили авторы, выявлены такие аспекты, как семейное положение жертв мошенничества (см. табл. 4) [28]. Некоторые ученые утверждают, что женатые люди более уязвимы, учитывая, что первыми жертвами того, кто пострадал от мошенничества с пирамидой, будут семья и друзья жертвы, которые не подозревают об обмане. Обычно жертвы финансовых мошенников — это люди, которые имеют небольшие сбережения и ищут способы инвестирования собственных средств, часто опираясь на советы семьи и друзей [54]. С другой стороны, одинокие люди более уязвимы в качестве жертв, чем состоящие в браке, учитывая социальную изоляцию и чувство одиночества.

Исследований профессионального статуса меньше, чем исследований других демографических характеристик (см. табл. 5) [28]. Однако приведенные в таблице исследования указывают на то, что большинство жертв работают по найму. Д. П. Шадель и К. Б. Швейцер-Пак (2007) разработали два исследования за два разных года, в которых были получены противоположные результаты [52]. Их работа также показала, что демографические факторы, такие как возраст, доход и уровень образования, могут влиять на

уязвимость человека к мошенничеству потребителей. Например, пожилые люди могут быть более уязвимы из-за снижения когнитивных способностей и недостаточного знакомства с технологиями, в то время как люди с более низким уровнем дохода и образования могут быть более восприимчивы к мошенническим схемам, которые предлагают быструю финансовую выгоду.

Таблица 4. Исследования жертв финансового мошенничества по семейному положению
Table 4. Research of financial fraud crime victims by marital status

Автор	Изучаемый период	Большинство жертв
Дж. Ли и О. Соберон-Феррер (1997)	1993	Не женатые
ААП (Американская ассоциация пенсионеров) (2007)	2006	Женатые
Д.П. Шадель, К.Б. Швейцер-Пак (2007)	2006-2007	Женатые
М.В. Зунзунеги и др. (2017)	2015-2016	Женатые
М. Делиема и др. (2020)	2016	Женатые
Д. Вуд и др. (2018)	2018	Не женатые
Ё. Кадоя и др. (2021)	2020	Не женатые

Таблица 5. Исследования жертв финансового мошенничества по профессиональному статусу
Table 5. Research of financial fraud crime victims by professional status

Автор	Изучаемый период	Большинство жертв
М. Локанан (2014)	1984-2008	Трудоустроенные
ААП (Американская ассоциация пенсионеров) (2007)	2006	Трудоустроенные
Д.П. Шадель, К.Б. Швейцер-Пак (2006)	2006	На пенсии и безработные
Д.П. Шадель, К.Б. Швейцер-Пак (2007)	2007	Трудоустроенные
М. Батон и др. (2014)	2014	Трудоустроенные
М.В. Зунзунеги и др. (2017)	2015-2016	Трудоустроенные

Кроме того, многие пострадавшие не желают сообщать о том, что они стали жертвой мошенничества. Почти 59% жертв, опрошенных Д. Ребовичем и Дж. Лайном, предпочли не сообщать о том, что стали жертвами [49]. Исследование, проведенное К. Р. Керли и Х. Коупсом (2002), направлено на изучение официальной реакции жертв мошенничества на их виктимизацию. Оно проводилось в США и включало опрос 1010 человек, которые сообщили, что стали жертвами мошенничества в течение предыдущих 12 месяцев. В ходе опроса использовалась структурированная анкета для сбора информации о типах мошенничества, с которыми сталкиваются жертвы, их восприятии своей виктимизации и их официальной реакции на преступление. Респондентов спрашивали об их контактах с различными официальными учреждениями, такими как полиция, банки и кредитные бюро, а также о типах полученных ими ответов. Результаты исследования показали, что только 10% жертв мошенничества обратились в полицию. Большинство жертв, которые не сообщили о преступлении, сочли, что оно было либо слишком незначительным, либо что полиция не сможет помочь. Исследование показало, что демографические данные жертв, такие как возраст, раса и уровень дохода, практически не влияли на решение сообщить о мошенничестве в полицию. Исследование также показало, что значительный процент жертв

мошенничества сталкивался с многочисленными попытками мошенничества в течение предыдущих 12 месяцев. В частности, 22% жертв столкнулись с двумя или более попытками мошенничества в течение этого периода. Авторы предполагают, что эти неоднократные случаи виктимизации могут указывать на необходимость дополнительной поддержки и разъяснительной работы с жертвами мошенничества [39, с. 19-35]. Ученые обнаружили, что тенденция не сообщать о мошенничестве имеет различные объяснения. Некоторые жертвы не понимают, куда им следует сообщать о мошенничестве. К. А. Мейсон и М. Л. Бенсон продолжили список факторов и указали, что низкое количество сообщений жертв связан с восприятием ответственности, уровнем потерь, социальными сетями и процессом правосудия [44, с. 511-524]. Некоторые жертвы избегают обращения в полицию, потому что хотят скрыть понесенные убытки от своих социальных сетей (семьи и друзей). Зачастую потерпевшие избегают сообщать о случаях, когда они понесли небольшие убытки или посчитали, что процесс уголовного правосудия не заслуживает доверия. Что касается процесса уголовного преследования, менее 50% американских жертв убеждены, что власти успешно раскроют дела о мошенничестве, в которых они пострадали. Согласно «теории права Блэка», склонность жертв мошенничества обращаться за помощью к правоохранительным органам зависит от культурного контекста. Например, приезжие скорее обратятся за помощью к закону, чем коренные жители.

Изучая виктимологию кибермошенничества — потребительского, благотворительного, инвестиционного и любовного — можно будет разработать более эффективные меры защиты граждан от подобных преступлений. Психологически профилируя жертв кибермошенничества, М. Т. Уитти использовала онлайн-анкету (10 723 человека, не ставших жертвами, и 1057 жертв). Участников спросили, не были ли они обмануты каким-либо образом в Интернете [56].

Вот к каким выводам пришла автор исследования:

Возраст: жертвы инвестиционного и потребительского мошенничества были старше, чем жертвы других видов мошенничества (например, фишинговые аферы).

Пол: женщины гораздо чаще становились жертвами потребительского мошенничества, а мужчины чаще становились жертвами мошенничества с инвестициями. В целом мужчины чаще подвергались мошенничеству, чем женщины.

Образование: в целом люди, имеющие образование, чаще подвергались мошенничеству, чем те, кто не имел образования.

Локус контроля: жертвы инвестиционного мошенничества набрали значительно более высокие баллы по внутреннему локусу контроля по сравнению с жертвами благотворительного и потребительского мошенничества. Жертвы с большей вероятностью, чем не потерпевшие, считали, что они контролируют исход событий в своей жизни.

Эмоциональная стабильность: жертвы мошенничества более эмоционально нестабильны по сравнению с теми, кто не стал жертвой [56].

Основываясь на этих результатах, автор предполагает, что, возможно, не существует универсального мошенничества, жертвой которого может стать любой человек, а скорее мошенничества нацелены на людей с определенными психологическими чертами и уязвимостями. Автор рекомендует, чтобы будущие исследования были сосредоточены на выявлении конкретных уязвимостей и разработке мер по снижению риска стать жертвами кибермошенничества. Полученные результаты подчеркивают важность понимания личности и психологических характеристик потенциальных жертв при разработке эффективных превентивных стратегий и возможностей практического обучения для снижения риска стать жертвой кибермошенничества.

В исследовании Д. Шейдела и К. Б. Швейцер-Пак (2007) отмечалось, что жертвами потребительского мошенничества часто становятся люди, которым не хватает знаний о работе финансовых рынков, которые чрезмерно уверены в своих способностях принимать обоснован-

ные финансовые решения, подвержены тактике убеждения мошенников и могут страдать от когнитивных искажений, таких как склонность к оптимизму и предвзятость суждений. Исследование также показало, что демографические факторы, такие как возраст, доход и уровень образования, могут влиять на уязвимость человека к потребительскому мошенничеству. В исследовании также подчеркивается важность психологических вмешательств, направленных на устранение индивидуальной уязвимости и когнитивных предубеждений, которые способствуют виктимизации [52].

Б. Л. Эльдадом и др. (2022) было выявлено, что жертвами финансового мошенничества в развивающихся странах часто становятся люди, не имеющие финансового образования, имеющие ограниченный доступ к банковским услугам и уязвимые в силу своего социально-экономического статуса. Исследование также показало, что определенные демографические группы, такие как пожилые люди и женщины, особенно подвержены финансовому мошенничеству. Авторы отмечают, что характеристики жертв финансового мошенничества в развивающихся странах формируются различными факторами, такими как культурные и социальные нормы, политическая и экономическая среда и институциональные рамки, регулирующие финансовые операции. Они утверждают, что директивным органам и организациям необходимо лучше понимать характеристики жертв финансовых махинаций в развивающихся странах, чтобы разработать эффективные стратегии предотвращения и вмешательства [28].

В последние годы финансовые махинации расширились и диверсифицировались, отражая растущую изобретательность мошенников и постоянную мотивацию жертв к быстрой высокой прибыли. Существует концептуальная путаница между финансовым и инвестиционным мошенничеством. Финансовое мошенничество включает в себя более широкий спектр незаконных действий, таких как фишинг, кража личных данных или мошенничество со страховкой, в то время как инвестиционное мошенничество является компонентом финансовой категории [35]. К наиболее распространенным инвестиционным махинациям относятся котельная, пирамида и схемы Понци. Схемы котельной, также называемые «мошенничеством в пресс-центре», включают в себя оказание давления на потенциальных жертв, чтобы они инвестировали в фиктивные или малоценные акции. Мошенники используют холодные звонки для жертв и представляют свой бизнес, используя поддельные ссылки. С другой стороны, пирамиды и схемы Понци похожи, но в случае пирамиды первым инвесторам необходимо привлекать новых инвесторов для получения прибыли [29]. Несмотря на диверсификацию мошеннических программ, схемы Понци сохранили свой первоначальный метод, к которому мошенники придумывали новые технологии и стратегии действий. Чарльз Понци разработал оригинальную схему в 1920-х гг., пообещав 50% прибыли тем, кто решит инвестировать в международные почтовые купоны. Это мошенничество включает в себя обещание высокой прибыли с ограниченными рисками или без них, в то время как мошенник использует средства в личных или незаконных целях. Оператор мошенничества платит старым инвесторам, используя часть средств, полученных от новых инвесторов, чтобы привлечь больше жертв [32]. Работа схем Понци и пирамид основана на постоянном притоке в схему новых участников. Следовательно, продолжительность работы сети прямо пропорциональна количеству жертв, а это означает, что чем больше число жертв, тем дольше существует пирамидальная структура.

Широкое использование кредитных карт в качестве основного метода транзакций является ярким примером цифровизации повседневной жизни и общества за последние пару десятилетий. Это внедрение также создает проблему мошенничества с кредитными картами, которое включает сложные стратегии и методы, используемые для кражи денег и активов. Авторы Б. Мытник и др. в своём исследовании проанализировали 3111 связанных документов в Scopus (см. рис. 1) [45].

Рис. 1. Статистика научных исследований мошеннической банковской сферы в базе данных Scopus по годам
Fig. 1. The statistics of scientific studies in fraudulent banking field in Scopus by year

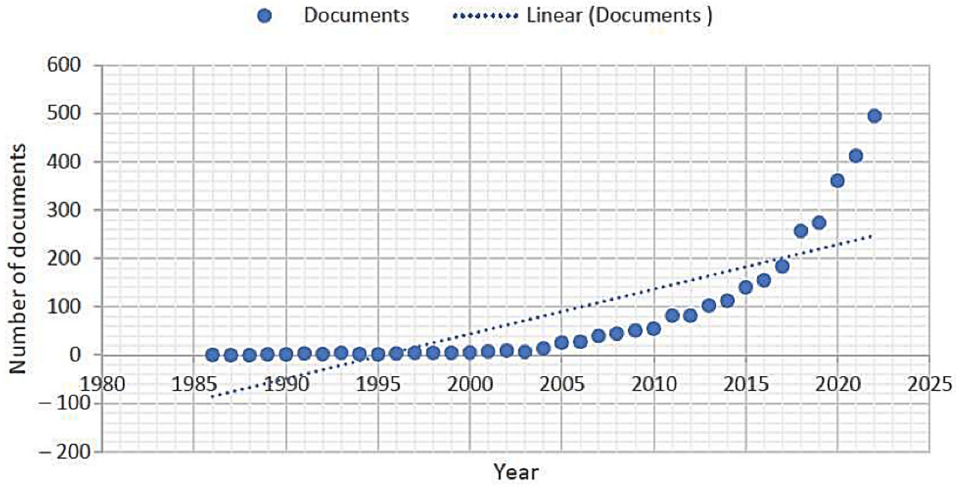

Рис. 1 показывает, что мошенничество в банковской сфере стало серьезной проблемой для финансовых учреждений и регулирующих органов во всем мире. Оно включает преднамеренные попытки отдельных лиц или организаций обмануть банки, финансовые учреждения или их клиентов с целью получения финансовой выгоды [45].

Существует два способа классификации мошенничества с кредитными картами: мошенничество с использованием приложений или поведенческое мошенничество, которые иногда также называют офлайн- и онлайн-мошенничеством соответственно. Мошенничество с приложениями часто связано с мошенничеством с идентификацией, поскольку обычно мошенники пытаются выпустить новые карты кредитных компаний, используя частную информацию других людей. Поведенческое мошенничество состоит из четырех различных действий, которые включают в себя кражу почты, кражу или утерю карт, подделку карт, мошенничество «отсутствие держателя карты» или мошенничество с банкротством. Мошенничество в связи с банкротством считается одним из самых сложных видов мошенничества для обнаружения и, как правило, предполагает использование людьми кредитной карты без намерения когда-либо вернуть остаток, а затем подачу заявления о личном банкротстве, как это было определено Гошем и Рейли в 1994 г. [33].

С быстрой цифровизацией повседневной жизни в Интернете доступно больше информации, которая впоследствии становится уязвимой для атак или использования преступниками и мошенниками. Р. Дж. Болтон и Д. Дж. Хэнд отметили, что в предыдущие годы опубликованная литература по обнаружению кредитных карт была недостаточной, так как ограниченный обмен идеями в области обнаружения мошенничества может привести к тому, что описывать методы обнаружения в открытом доступе может быть нелогичным. Это может предоставить знания и информацию, которые могут быть использованы для разработки новых инструментов и техник обхода этих методов обнаружения. Как обсуждалось ранее, за необнаруженное мошенничество также приходится платить с течением времени, а это означает, что ценность обнаружения мошенничества зависит от времени. Чем раньше будет обнаружена мошенническая деятельность, тем меньше потенциальные потери физических лиц и компаний [19, с. 235-255].

Наиболее распространенные виды мошенничества нацелены на граждан через поддельные электронные письма, текстовые сообщения, голосовые вызовы. Используемые мошенниками методы могут быть разные, например:

- Неожиданно связались по телефону, электронной почте, тексту, прямому сообщению или всплывающему окну с запросом личной информации или денег;
- Гражданин вынужден действовать немедленно с помощью тревожного телефонного звонка, электронного письма или сообщения, которое играет с его эмоциями. Мошенники могут представиться сотрудником знакомой организации, например сотрудником банка, уполномоченного органа, даже назвать существующее имя, и заявить, что возникла проблема, требующая немедленного решения;
- Просят оплатить необычным способом, например подарочными картами, биткойнами, предоплаченными дебетовыми картами или цифровой валютой, для устранения мошенничества;
- Просят предоставить личную информацию или информацию об учетной записи, такую как код подтверждения учетной записи, номер банковского счета или PIN-код;
- Предложили бесплатный продукт или возможность «быстро разбогатеть», которая кажется слишком хорошей, чтобы быть правдой.

Если гражданин разрешает перевод или отправляет деньги мошеннику, банки зачастую мало что могут сделать, чтобы вернуть деньги [18].

Современные технологии не только приносят вред, то есть благодаря им мошенники могут обманывать людей, но также помогают предотвращать подобное мошенничество. Например, разработке искусственного интеллекта для распознавания мошеннических банковских операций в последние годы уделяется значительное внимание. Системы на основе искусственного интеллекта могут эффективно выявлять и предотвращать мошеннические действия в режиме реального времени, обеспечивая значительное преимущество по сравнению с традиционными методами обнаружения мошенничества.

Опыт разных стран в борьбе с финансовым мошенничеством граждан варьируется в зависимости от таких факторов, как уровень их экономического развития, правоприменительная политика и технологические достижения. Например, развивающиеся страны часто имеют более слабую нормативно-правовую базу для финансовых учреждений и более низкий уровень осведомленности граждан о том, как защитить себя от финансового мошенничества. Такие условия делают эти страны привлекательными мишенями для лиц, совершающих финансовые преступления.

Напротив, развитые страны добились большего успеха в борьбе с финансовым мошенничеством путем введения строгих нормативных актов, внедрения передовых технологий мониторинга и частого проведения государственных образовательных программ для повышения осведомленности граждан о потенциальных рисках финансового мошенничества. К примеру, в некоторых странах, таких как Канада, были созданы специализированные отделы в государственных учреждениях, которые занимаются расследованием случаев финансового мошенничества, в то время как в других странах, таких как Соединенное Королевство, используются сложные автоматизированные системы обнаружения.

Несмотря на согласованные усилия по борьбе с финансовым мошенничеством во всем мире, в некоторых странах по-прежнему наблюдается высокий уровень этих преступлений в силу различных факторов. Высокий уровень бедности, политическая нестабильность и неадекватные правоохранительные меры являются распространенными причинами высокого уровня финансового мошенничества во многих странах. Нестабильность политических режимов также способствует коррупции и мошенничеству, так как контролирующие органы, отвечающие за предотвращение этих преступлений, могут быть вовлечены в коррупционные схемы. Это позволяет мошенникам уклоняться от ответственности и приводит к дальнейшему распространению этих проблем.

Страны, которые со временем успешно сократили масштабы финансового мошенничества, внедрили современные технологии и комплексные стратегии, которые поддерживают информированность граждан и правоохранительных органов, а кроме того, они сотрудничают с другими странами для достижения лучших результатов в борьбе с этой проблемой.

Не существует единого решения проблем, связанных с финансовым мошенничеством, и правительствам стран приходится применять множество подходов с учетом разных социально-экономических условий. Необходимо постоянно обновлять правила, проводить просветительскую работу среди граждан и принимать комплексные меры для снижения рисков и обеспечения безопасности финансовых операций. Только такой подход может пресечь финансовые мошенничества и защитить интересы населения.

Основные обстоятельства, приводящие к увеличению числа жертв финансового мошенничества, связаны с экономическими трудностями. Многие жертвы состоят в браке и, учитывая как финансовые, так и семейные обстоятельства, нуждаются в деньгах, чтобы поддерживать свои семьи в краткосрочной перспективе [27, с. 85-92]. Индийские жертвы ищут дополнительные средства, чтобы улучшить свой уровень жизни или построить финансовую базу для повышения собственного экономического положения. Экономические условия и бедность также способствуют финансовому мошенничеству в Нигерии [37, с. 72-90]. Отсутствие сочувствия к другим и жадность являются факторами, поддерживающими тенденцию быть привлеченными финансовыми мошенниками в Китае, Нигерии и Латинской Америке.

Согласно исследованию Лаборатории Касперского, Россия занимает второе место среди стран с наибольшим количеством кибератак в мире, подвергаясь более чем в два раза большему количеству атак по сравнению с Францией и Германией вместе взятыми. Эта тенденция была вызвана российскими хакерами, которые продолжают разрабатывать новые методы кражи конфиденциальных данных и денежных средств.

Финансовое мошенничество продолжает представлять значительную угрозу для экономики России. По данным Центрального банка России (ЦБР), объем мошеннических действий, выявленных в банковском секторе страны, увеличился на 26% в первом полугодии 2021 г. по сравнению с аналогичным периодом 2020 г.

Проблема несанкционированных банковских операций в России вызывает растущую озабоченность как у правительства, так и у граждан. С учетом растущего числа жалоб на несанкционированные банковские операции становится ясно, что проблему необходимо решать немедленно. Объем таких операций вызывает озабоченность, особенно в отношении дистанционного банковского обслуживания физических лиц, и их продолжение может нанести значительный ущерб экономике в целом. Поэтому необходимо принять срочные меры для пресечения несанкционированных банковских операций. На рис. 2 изображена статистика несанкционированных банковских операций в России в третьем квартале 2022 г., подготовленная Отделом статистических исследований (Statista Research Department).

С июля по сентябрь 2022 г. объем несанкционированных банковских операций, совершенных с использованием ДБО (дистанционного банковского обслуживания) для физических лиц в России, составил более 2,7 млрд рублей. Сумма мошеннических операций, проведенных с использованием банкоматов и платежных терминалов, составила около 390 млн рублей.

Существуют различные виды несанкционированных банковских операций, включая отмывание денег, мошенничество и другие финансовые преступления. В этой деятельности часто участвуют отдельные лица или организации, пытающиеся скрыть свои незаконные доходы, направляя их по казалось бы законным каналам. Они пользуются лазейками в существующих нормативных актах, слабым правоприменением и коррупционной практикой.

Несанкционированные банковские операции имеют более широкие последствия, чем простое нарушение законодательства. Они подрывают доверие к финансовой системе и создают значительные риски для экономической стабильности и национальной безопасности. Распространение таких операций приводит к искажению механизмов ценообразования, неэффективности рынка и увеличению системных рисков для всего финансового сектора. Поэтому необходимо принимать меры для предотвращения несанкционированных банковских операций.

Рис. 2. Объем несанкционированных банковских операций в России в 3 квартале 2022 г. (в млн российских рублей)

Fig. 2. The volume of unauthorized banking transactions in Russia in the 3rd quarter of 2022 (in mln of Russian rubles)

Для эффективного решения проблемы необходимо принимать еще больше мер. Улучшение мер надзора и прозрачности позволит выявлять и предотвращать подозрительную деятельность на ранних стадиях, а более строгие меры наказания могут служить сдерживающим фактором для потенциальных мошенников. В целом борьба с незаконными финансовыми операциями требует совместных усилий всех уровней правительства и гражданского общества и должна быть постоянной.

Представители Альфа-банка и Газпромбанка рассказали РБК (российский мультимедийный холдинг РосБизнесКонсалтинг), что в феврале-марте 2022 г. активность кибермошенников снизилась. Почта Банк заметил, что мошеннические телефонные звонки стали происходить реже, а случаи кражи денег со скомпрометированных карт, владельцы которых оплачивали онлайн-покупки небезопасными методами, без ввода одноразового пароля из СМС, увеличились на 40%. ВТБ, наоборот, зафиксировал рост мошенничества. Нередко по телефону гражданам стали предлагать перевести деньги на «сейф» или «сохранить» депозит или валюту через перевод на другой счет [9].

Первый зампред комитета Госдумы по экономической политике Н. Арефьев отметил, что падение уровня жизни стало одной из причин роста финансовых мошенничеств в России на 85%, по сообщению Центробанка. В связи с этим депутат призвал повышать уровень жизни населения и отметил недостаточный уровень экономической грамотности россиян [7].

Центробанк опубликовал отчет, в котором указывается, что количество мошеннических организаций в России увеличилось на 85% в 2022 г. по сравнению с предыдущим годом. Общее число таких компаний составило около пяти тысяч, из которых две тысячи являются финансовыми пирамидами, 1,2 тысячи — незаконными профессиональными рыночными участниками и 1,7 тысячи черных кредиторов. Большинство организаций обманным путём завлекали жертв в сети Интернет. В целом за 2022 г. злоумышленники провели меньше мошеннических пере-

водов, однако украли больше денег, чем в 2021 г. Это объясняется ростом электронных переводов. В этом году банковские организации возмещали своим клиентам всего лишь 4,4% от потерь, или 618,4 млрд руб. Этот показатель является самым низким с 2019 г. Если 2022 году банки возмещали клиентам до 6,8 %, или 920,5 млн руб., то в 2020 г. их возмещение составило до 11,3 %, или 1,1 млрд руб., а в 2019 г. до 15%. Такой уровень возмещения объясняется сохранением высокой доли социальной инженерии, когда граждане переводят свои сбережения по просьбам мошенников или раскрывают им свои личные данные. В таких случаях закон освобождает банки от ответственности за потерю денег клиента. За 2022 год злоумышленникам удалось украсть у банковских клиентов около 14,1 млрд руб., что является самым высоким показателем минимум с 2019 г. До этого ЦБ учитывал в статистике мошеннических операций только транзакции по картам. Сейчас в общую статистику этих преступлений включаются все транзакции, проведенные с помощью электронных средств платежей. В рассуждении Центробанка о таком высоком уровне мошенничества оправдывается активное развитие новых дистанционных сервисов оплаты и рост объема денежных переводов при использовании электронных средств платежа. В 2022 г. банковские клиенты перевели около 1,4 квадриллиона руб., что является рекордным значением на фоне годового роста до 39% [1].

В 2022 г. Банк России провел опрос о степени удовлетворенности финансовых услуг и сталкивался с людьми, которые были наиболее подвержены обману. Банк России составил портрет гражданина, который подвержен мошенничеству: это работающий мужчина среднего возраста (от 25 до 44 лет) среднего уровня дохода и образования, проживающий в городе и активно использующий онлайн-банковские услуги.

Более половины опрошенных (58,2%) не сталкивались с мошенничеством. 3,5% респондентов являются жертвами аферистов, а 31,8% человек не теряли средства в результате кражи. Еще 6,5% респондентов не знали, как ответить на этот вопрос [10].

В России наблюдается и новый способ финансового мошенничества с жильем. Преступники получают доверие продавцов квартир, представляясь сотрудниками банка, агентами по недвижимости или представителями правоохранительных органов, и убедительно обманывают их. Они сообщают жертвам о попытке мошенников вывести средства со счета, на который поступал доход от продажи жилья. Затем злоумышленники просят перевести эти деньги на безопасный счет. Целью аферистов является получение достаточной информации для вывода денег.

Аналогичным образом зарубежные страны переживают всплеск финансового мошенничества из-за технологических достижений. Например, в США кража личных данных является одним из наиболее значительных видов финансового мошенничества, ежегодно обходящегося жертвам в миллиарды долларов. Федеральному резервному банку Нью-Йорк (ФРБ) стало известно о мошенничестве с авансовыми платежами, в котором неправомерно использовались имена реальных или вымышленных должностных лиц ФРБ Нью-Йорка. Мошенники выдавали себя за президента ФРБ Нью-Йорка Джона Уильямса, директора ФРБ Нью-Йорка по управлению рисками Джоша Розенберга и других лиц в общении с жертвами мошенничества. По данным компании «Robokiller», которая предлагает услугу блокировки звонков мошенников для мобильных телефонов, в 2022 г. пользователи телефонов в США получили 157 млрд робототекстов, более 440 текстов на человека, что на 80% больше, чем в 2021 г. А в 2022 г., согласно данным Федеральной торговой комиссии США, более 321 000 американцев сообщили о том, что стали жертвами мошенничества с использованием телефонов, с общими потерями более 326 млн долларов [34]. Проблема стала настолько серьезной, что в прошлом месяце федеральное правительство США потребовало, чтобы компании мобильной связи начали блокировать спам-сообщения. Федеральная комиссия по связи назвала эту меру первым из запланированных шагов по борьбе с телефонным мошенничеством. Некоторые банки призва-

ли граждан использовать системы электронных переводов, в том числе Zelle (система денежных переводов в США) [31].

Крупная австралийская четверка банков делает недостаточно для защиты клиентов от мошенничества и может даже способствовать «дальнейшим бедствиям для клиентов», подчеркивается в новом отчете австралийской финансовой службы. Исследование, опубликованное Австралийской комиссией по ценным бумагам и инвестициям, призывает финансовые учреждения улучшить методы борьбы с мошенничеством. Анализ показал, что убытки от мошенничества для крупных клиентов банка в 2022 г. финансовом году превысили 550 млн долларов; пострадали более 31 700 клиентов. Отмечается, что за последние несколько лет были вложены значительные средства в усилия по борьбе с мошенничеством и реализован ряд инновационных и позитивных инициатив [17].

В Соединенном Королевстве (Великобритания) Управление национальной статистики сообщило, что в период с марта 2019 г. по март 2020 г. в Англии и Уэльсе было зарегистрировано 3,8 млн случаев мошенничества. Согласно отчету, количество случаев мошенничества с банковскими и кредитными счетами увеличилось на 157% по сравнению с предыдущим годом. Правительство Великобритании признает угрозу подобных преступлений и активно сотрудничает с такими организациями, как Financial Fraud Action UK (Действие по борьбе с финансовым мошенничеством в Великобритании), для борьбы с этими проблемами. В Великобритании риски мошенничества были выявлены в начале двадцать первого века, и требовались ответные меры национальной политики. В борьбе с мошенничеством власти Великобритании применяют не только полицейские методы. В целях предотвращения финансового мошенничества большое внимание уделяется аудиту и обмену информацией. В 2011 г. была представлена стратегия «Борьба с мошенничеством вместе», которая охватывала меры реагирования как государственного, так и частного секторов. Количество государственных инициатив и организационных изменений в области борьбы с мошенничеством стало настолько велико, что отслеживать их стало затруднительно. Власти и комиссии были ликвидированы, а обязанности перераспределены, что не позволило эффективно пересмотреть стратегию и оценить ее действенность по всей стране. Поэтому неизвестно, какое воздействие эта стратегия оказала или могла бы оказать на реальный уровень мошенничества. Согласно выводам авторов, стратегия в области борьбы с мошенничеством должна развиваться и адаптироваться, а не быть навязываемой исключительно сверху вниз. Роль в реализации стратегии должна принадлежать органу, который обладает полномочиями, ресурсами и поддержкой для обеспечения правильного руководства, а также механизмов обратной связи, необходимых для пересмотра и адаптации стратегии в соответствии с изменяющимися обстоятельствами. Для этого необходимо постоянно уделять внимание вопросам борьбы с мошенничеством со стороны центрального правительства [41, с. 285-291].

Подобная ситуация характерна и для Соединенных Штатов Америки. В июле 2021 г. президент Джо Байден опубликовал меморандум, направленный на борьбу с атаками программ-вымогателей в США. Согласно данным Федеральной торговой комиссии, только в 2020 г. американцы потеряли более 3,3 млрд долларов по причине мошенничества — это почти на 1,5 млрд долларов больше, чем в предыдущем году. Используя передовые технологии, мошенники нацеливаются на своих жертв, будь то физические лица или предприятия в США. Они считают, что достижение успеха может привести к миллиардным прибылям. Согласно отчету Центра жалоб на интернет-преступления, число жалоб на интернет-преступления в США составило 467 361, а заявленный ущерб превысил 3,5 млрд долларов, что на 30% больше, чем годом ранее. Эти потери связаны с различными действиями, такими как компрометация деловой электронной почты для осуществления несанкционированных переводов средств, случаи мошенничества с идентификацией, включая поддельные чеки и заявки на кредитные карты, и мн. др. [55]. Чтобы смягчить последствия финансового мошенниче-

ства для граждан, многие страны ввели различные средства идентификации и аутентификации. В США многофакторная аутентификация (МФА) стала важным инструментом для предотвращения мошеннических действий, связанных с кражей конфиденциальных данных или несанкционированным доступом к учетным записям пользователей.

Индия также страдает от проблем с финансовым мошенничеством — фишинговые электронные письма являются одной из серьезных проблем, с которыми сталкиваются граждане Индии, приводя к огромным денежным потерям. Низкий уровень финансовой грамотности — один из основных факторов, способствующих тому, что в развивающихся странах люди становятся жертвами финансовых мошенничеств. Большинство жертв из Индии были женатыми мужчинами, считавшими, что финансовые решения принимают мужчины в семье. Что касается образования и профессионального статуса, то большинство жертв в Индии обычно трудоустроены и имеют формальное образование (академическую степень или выше). Образованные люди более склонны становиться жертвами финансового мошенничества, учитывая, что в последнее время мошенничество в Индии было основано на криптовалютах. Поэтому инвестировать в них пытались только те, кто читал о криптовалютах.

В Боливии жертвами являются мелкие вкладчики, которые ищут альтернативные варианты инвестирования своих небольших сбережений. Потенциальными жертвами являются безработные с минимальной заработной платой. Такая же ситуация справедлива для развивающихся стран Латинской Америки. В соответствии с финансовой грамотностью в Малайзии можно выделить два типа жертв. Многие люди в Малайзии не имеют достаточных знаний в области финансов, их легко обманывают, так как они не понимают принципы финансирования и предпочитают инвестировать в финансовые схемы из-за незнания [23].

Аналогичная ситуация имеет место в Кении, где мошенничество продолжает быть серьезной проблемой, несмотря на предпринимаемые меры для борьбы с мошенничеством. Граждане Кении подвергаются различным формам мошенничества — от кражи данных кредитных карт посредством общественных Wi-Fi сетей до мошенничества с заменой SIM-карт, когда злоумышленники переводят телефонные номера на другие мобильные устройства и наносят личный и финансовый ущерб жертвам.

Финансовые махинации начали процветать и в Китае в последние десятилетия, что власти определили это явление как реальную угрозу общественному порядку. Одной из причин расцвета мошенничества является слабое регулирование финансовых структур, работающих в сети, наряду с жадностью и желанием разбогатеть, которые стали основной движущей силой китайского общества [26]. В Китае физические лица являются легкой добычей для мошенников, поскольку китайские рынки открылись в 1990-х гг. и поэтому у населения мало опыта управления капиталом, знакомства с финансовыми рисками и умения выбирать финансовые продукты. Кроме того, повышенный уровень финансовой грамотности выступает защитным фактором от того, чтобы не стать жертвой финансового мошенничества. Несмотря на финансовую грамотность, акцент делается на риск-ориентированность в прогнозировании жертв финансового мошенничества для Китая, которые скорее относят себя к оптимистичным с высокой склонностью к риску. Эта тенденция особенно ярко выражена среди тех, кто не раз попадался на мошенников. В Китае люди старше 60 лет более подвержены риску стать жертвами финансовых мошенников, так как многие из них ищут способы повышения своего пенсионного дохода, инвестируя в финансовые схемы. Экономические проблемы могут стать большой нагрузкой для людей, на пороге выхода на пенсию или пенсионеров, которые ожидают значительных медицинских расходов и затрат на проживание. Именно поэтому люди этой возрастной группы стремятся к прибыльным краткосрочным инвестициям, что может привести к тому, что они станут жертвами мошенничества. Большинство китайских жертв финансовых схем были женщинами, поскольку

во многих китайских семьях женщины берут на себя управление финансовыми делами семьи. Однако общая сумма, вложенная женщинами в финансовые схемы, была почти равна общей сумме, вложенной мужчинами. Женщины, как правило, вкладывали несколько раз небольшие суммы, в то время как мужчины были более склонны вкладывать большую сумму сразу. Таким образом, мужчины, по-видимому, более склонны к риску, чем женщины, [23].

Несмотря на плохие экономические условия, выявленные в Нигерии, жадность связывают с одним из основных мотивов возникновения финансовых схем. Ожидание получения высокой прибыли за короткий период было одним из мотивирующих факторов для участия в финансовых схемах наряду с низким и ухудшающимся уровнем жизни в Нигерии. Когда многие участники получили высокие краткосрочные доходы, другие были очарованы доходностью и присоединились к мошенничеству. Существующие и новые инвесторы сосредоточились на доходах и не задавались вопросом, как они были получены [23].

Исследования финансового мошенничества проводились во всем мире, и различные страны разрабатывали собственные определения и подходы к борьбе с ним. Россия предприняла шаги по борьбе с финансовым мошенничеством, используя законы, направленные на защиту своих граждан. Однако существует разрыв между тем, как эта концепция понимается на местном и международном уровнях.

С другой стороны, зарубежные страны, такие как Соединенные Штаты Америки и европейские государства, имеют более полное представление о финансовом мошенничестве. Это связано с различиями в рыночной экономике, законодательстве и культуре доверия между гражданами и властями. В США и Европе существуют более развитые финансовые системы, такие как фондовые рынки, что может создавать потребности в более высоком уровне понимания финансовых мошенничеств. Кроме того, они внедрили более жесткие законы и правила с целью предотвращения и пресечения финансового мошенничества. В России ситуация отличается, что связано с недостаточной развитостью финансовой системы, наличием коррупции, а также с другими социальными, экономическими и культурными факторами. Кроме того, интернет-инфраструктура в России менее развита по сравнению с западными аналогами.

В заключение следует отметить, что проблема, связанная с финансовыми преступлениями, основанными на технологиях, требует от правительств единого подхода, подкрепленного кампаниями по просвещению общественности относительно того, как преступники реализуют эти виды мошенничества. Хотя никакие инструменты или структуры предотвращения не могут гарантировать стопроцентную эффективность, внедрение таких мер, как МФА, биометрических методов входа в систему и т.д., значительно снижает вероятность потенциальных атак, что приводит к снижению потерь как для частных лиц, так и для предприятий.

ВЫВОДЫ И ЗАКЛЮЧЕНИЕ

Финансовое мошенничество затрагивает людей по всему миру, и многие становятся жертвами все более изощренных преступных схем, направленных на использование их финансов. Технологии продолжают развиваться, поэтому жертвы и правоохранительные органы должны оставаться бдительными и действовать заблаговременно для выявления финансовых мошеннических действий.

Все больше случаев финансового мошенничества происходит по всему миру, и в настоящее время оно имеет большой потенциал для распространения из-за непрочной экономической ситуации и отсутствия финансовой грамотности среди граждан в нашей и других странах. Жертв привлекают финансовые махинации в разных контекстуальных обстоятельствах (финансовых и семейных). В то время как финансовые обстоятельства относятся к имеющимся финансовым ресурсам, финансовому положению и социальным связям, семейные обстоятельства предполагают необходимость обеспечить финансовое будущее семьи.

Для противодействия растущей угрозе финансового мошенничества в России необходимо создать эффективные стратегии, которые будут направлены на уменьшение его негативного влияния на отдельных граждан и экономику в целом. Важным средством достижения этой цели является проведение масштабных информационных кампаний, которые будут уведомлять общественность о рисках мошенничества и обучать людей способам защиты.

Число жертв можно уменьшить за счет ужесточения правительственных постановлений, касающихся финансов и конфиденциальной информации граждан, и увеличения информирования населения и профилактических мероприятий, особенно среди людей с низким доходом. Более того, государство должно найти инструменты для улучшения условий жизни своих граждан и снижения экономических и социальных негативных последствий в период экономической неопределенности, чтобы жертвы больше не интересовались мошенническими способами выигрыша.

Кроме того, регулирующие органы должны гарантировать соблюдение строгих правил, которые устанавливают более жесткие требования к аутентификации физических и юридических лиц, осуществляющих транзакции с высоким уровнем риска. Меры могут включать дополнительную авторизацию с защищенным паролем или биометрическую аутентификацию, которые обеспечивают безопасность конфиденциальной информации, которыми многие граждане не пользуются.

Кроме того, важно инвестировать в инфраструктуру кибербезопасности, чтобы обеспечить систему раннего предупреждения о кибератаках, которые могут привести к финансовому мошенничеству. Передовые аналитические инструменты, такие как искусственный интеллект, могут помочь обнаружить аномалии и подозрительные модели поведения, типичные для финансовых мошенничеств.

Чтобы не стать жертвой финансового мошенничества, мы собрали рекомендации, которые помогут снизить уровень мошенничества в стране:

- Повышение осведомленности общественности — проведение образовательных кампаний о рисках финансового мошенничества;
- Повышение уровня образования — разработка программ как для взрослых, так и для общеобразовательных учреждений, способствующих повышению финансовой грамотности, снижению уровня невежества и автономии, развитию навыков раннего принятия решений и развитию когнитивной беглости;
- Разработка инструментов для уменьшения инсайдерского мошенничества — большинство случаев финансового мошенничества может произойти из-за инсайдерской информации, следовательно, использование методов тщательного изучения неправомочных действий агентов, поможет уменьшить нечестное поведение;
- Применение строгих мер регулирования: правительствам следует усилить меры регулирования для борьбы с финансовым мошенничеством, такие как разработка процессов и структур для выявления и снижения финансовых рисков;
- Создание центрального органа для надзора за всеми аспектами мер по борьбе с финансовым мошенничеством путем координации с правоохранительными органами и финансовыми регуляторами;
- Введение обязательных требований к отчетности для финансовых учреждений, которые предполагают уведомление соответствующих органов в течение нескольких дней после обнаружения любой подозрительной деятельности;
- Внедрение алгоритмов шифрования, поскольку интернет-банкинг становится все более популярным, предоставляя хакерам больше возможностей для кражи личных данных с помощью различных кибератак;
- Усиление меры кибербезопасности: между банками или предприятиями и их клиентами необходимо внедрить более строгие протоколы кибербезопасности, гарантирующие, что вирусы не попадут на компьютеры клиентов и хакеры не смогут получить доступ, в ином случае банк или предприятие должны брать на себя полную ответственность за несохранение, что необходимо урегулировать законом;

• Укрепление сотрудничества с другими государственными учреждениями: правоохранительные органы должны сотрудничать с правительством и участниками частного сектора в обмене информацией, касающейся мошеннической деятельности и передачи информации из одного региона в другой;

• Расширение сотрудничества с Интерполом: международное сотрудничество необходимо для отслеживания и пресечения деятельности глобальных сетей, занимающихся финансовыми преступлениями, поскольку нет географических ограничений, связанных с границами Интернета;

• Использование новых карточных технологий, таких как EMV, может ограничить определенные виды мошенничества в сфере розничных банковских услуг как для потребителей, так и для операторов;

• Поощрение в создании схем информирования, при которых те, кто что-либо подозревает, могут сообщать об этом анонимно, не опасаясь возмездия, таким сторонам следует предоставлять поощрения после выявления фактов/расследования их заявлений;

• Проведение периодической оценки эффективности систем регулирования и избирательной практики (регистрации избирателей, правила голосования, подсчет и обработка голосов, контроль за финансированием кампаний и т. д.) для проверки их оптимальной работы и достижения ожидаемых значимых результатов. Финансовые страховщики также должны выполнять эту оценку в различных сферах и при внедрении политики.

Несмотря на то, что современные технологии облегчили нашу жизнь, они также сделали ее более уязвимой перед мошенниками. Чтобы избежать финансовых мошенничеств, необходимо быть бдительными, следить за событиями и принимать соответствующие меры предосторожности для снижения рисков. Развитие современных технологий продолжает подпитывать и развитие финансового мошенничества во всем мире. Россия, в частности, сталкивается со значительной угрозой, исходящей от киберпреступников, стремящихся обмануть как предприятия, так и частных лиц. Для снижения этих рисков и повышения устойчивости финансового сектора к будущим угрозам необходимы эффективные стратегии, такие как кампании по просвещению общественности, ужесточение правил и передовые системы кибербезопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Банк России. Обзор операций, совершенных без согласия клиентов финансовых организаций. Электронный ресурс: https://www.cbr.ru/analytics/ib/operations_survey_2022/ (дата обращения 10.05.23).
2. Батурин Ю.М., Жодзишский А.М. (1991). Компьютерная преступность и компьютерная безопасность. Электронный ресурс: https://www.elibrary.ru/item.asp?id=20854436 (дата обращения 10.05.23).
3. Брусникина А.Е. (2015). Мошенничество на финансовом рынке и способы его предупреждения. Электронный ресурс: https://cyberleninka.ru/article/n/moshennichestvo-na-finansovom-rynke-i-sposoby-ego-preduprezhdeniya (дата обращения 10.05.23).
4. Головинов О.Н., А.В. Погорелов (2016). Киберпреступность в современной экономике: состояние и тенденции развития. Электронный ресурс: https://cyberleninka.ru/article/n/kiberprestupnost-v-sovremennoy-ekonomike-sostoyanie-i-tendentsii-razvitiya (дата обращения 10.05.23).
5. Дадалко В.А. (2017). Методы противодействия рискам кассового мошенничества как инструмент обеспечения экономической безопасности организации. Электронный ресурс: https://cyberleninka.ru/article/n/metody-protivodeystviya-riskam-kassovogo-moshennichestva-kak-instrument-obespecheniya-ekonomicheskoy-bezopasnosti-organizatsii (дата обращения 10.05.23).
6. Маронова Ж.Е. (2019). Мошенничество на финансовом рынке и способы его предупреждения. Электронный ресурс: https://cyberleninka.ru/article/n/moshennichestvo-na-finansovom-rynke-i-sposoby-ego-preduprezhdeniya-1 (дата обращения 10.05.23).

7. Парламентская газета (2023). Издание Федерального Собрания Российской Федерации. Электронный ресурс:https://www.pnp.ru/social/2013/04/10/nikolay-arefev-gosudarstvo-prakticheski-zanimaetsya-otyomom-deneg-u-naseleniya.html (дата обращения 10.05.23).
8. Петрякова Л.А. (2020). Проблемы квалификации мошенничества в банковской сфере. Электронный ресурс: https://cyberleninka.ru/article/n/problemy-kvalifikatsii-moshennichestva-v-bankovskoy-sfere (дата обращения 10.05.23).
9. РБК (2022). Как изменились схемы банковского мошенничества из-за санкций? URL: https://www.rbc.ru (дата обращения 10.05.23).
10. РБК (2022). ЦБ раскрыл данные об инцидентах при переводе средств. URL: https://www.rbc.ru (дата обращения 10.05.23).
11. Ревякин С.В. (2018). Профилактика мошенничества с использованием современных электронных средств коммуникации. Электронный ресурс: https://cyberleninka.ru/article/n/profilaktika-moshennichestva-s-ispolzovaniem-sovremennyh-elektronnyh-sredstv-kommunikatsii (дата обращения 10.05.23).
12. Фойницкий, И. Я. Мошенничество по русскому праву / И. Я. Фойницкий. — Санкт-Петербург: Типография товарищества Общественная польза, 1871. — 551 с. — Режим доступа: по подписке. — URL: https://biblioclub.ru/index.php?page=book&id=71367 (дата обращения 10.05.23).
13. Чикишева Н.А. (2009) Криминологическая характеристика личности женщины-мошенницы. Электронный ресурс: https://cyberleninka.ru/article/n/kriminologicheskaya-harakteristika-lichnosti-zhenschiny-moshennitsy (дата обращения 10.05.23).
14. AARP (American Association of Retired Persons) (1999). Consumer behavior, experiences and attitudes: A comparison by age groups. New Jersey: Princeton Survey Research Associates. URL: https://www.aarp.org (дата обращения 10.05.23).
15. AARP (American Association of Retired Persons) (2007). Stolen futures: An AARP Washington survey of investors and victims of investment fraud. Washington DC: AARP. URL: https://www.aarp.org (дата обращения 10.05.23).
16. Achim M.V., Borlea S.N. McGee R.W., Muresan G.M., Safta I.L., Vaidean V.L. (2020). inancial Crime: A Literature Review. URL: https://www.researchgate.net/publication/366090442_Financial_Crime_A_Literature_Review (дата обращения 10.05.23).
17. ASIC (Australian Securities & Investments Commission (2023). URL: https://asic.gov.au/about-asic/news-centre/find-a-media-release/2023-releases/23-101mr-asic-calls-for-improved-approaches-to-scams-as-major-bank-customers-report-over-550-million-in-scam-losses/ (дата обращения 10.05.23).
18. Bank of America (2023). How to Avoid Scams. URL: https://www.bankofamerica.com (дата обращения 10.05.23).
19. Bolton R.J., D.J. Hand (2002). Statistical fraud detection: A review. Statistical Science, 17 (3) (2002), pp. 235-255. URL: https://www.jstor.org/ (дата обращения 10.05.23).
20. Bossler A.M., Berenblum T. (2019). Introduction: new directions in cybercrime research. URL: https://www.researchgate.net/publication/337357079_Introduction_new_directions_in_cybercrime_research , (дата обращения 10.05.23).
21. Burke, J., Kieffer, C., Mottola, G., and Perez-Arce, F. (2022). Can educational interventions reduce susceptibility to financial fraud? J. Econ. Behav. Organ. 198, pp. 250–266. URL: https://scholar.google.com (дата обращения 10.05.23).
22. Button, M., Lewis, C., and Tapley, J. (2009). Fraud typologies and the victims of fraud: Literature review. London: National Fraud Authority URL: https://researchportal.port (дата обращения 10.05.23).
23. Cheng, H. (2016). Financial crime in China: Developments, Sanctions, and The Systemic Spread of Corruption. New York: Palgrave Macmillan. URL: https://scholar.google.com/scholar (дата обращения 10.05.23).
24. Copes, H., Kerley, K. R., Mason, K. A., and Van Wyk, J. (2001). Reporting behavior of fraud victims and Black's theory of law: an empirical assessment. Justice Q. 18, pp. 343-363. URL: https://www.tandfonline.com/doi (дата обращения 10.05.23).

25. Deliema, M., Shadel, D., and Pak, K. (2020). Profiling victims of investment fraud: mindsets and risky behaviors. J. Consum. Res. 46, pp. 904-914. URL: https://academic.oup.com (дата обращения 10.05.23).
26. Dor, O. (2017). Why do the Chinese continue to fall into the trap of pyramid scams? URL: https://www.calcalist.co.il (дата обращения 10.05.23).
27. Dreber, A., Apicella, C. L., Eisenberg, D. T., Garcia, J. R., Zamore, R. S., Lum, J. K., et al. (2009). The 7R polymorphism in the dopamine receptor D4 gene (DRD4) is associated with financial risk taking in men. Evol. Hum. Behav. 30, pp. 85-92. URL: https://doi.org/10.1016/j.evolhumbehav.2008.11.001 (дата обращения 10.05.23).
28. Eldad Bar Lev, Liviu-George Maha and Stefan-Catalin Topliceanu (2022). Financial frauds' victim profiles in developing countries. URL: https://www.frontiersin.org (дата обращения 10.05.23).
29. Europol. (2017). European Union serious and organised crime threat assessment (SOCTA). Crime in the age of technology. The Hague: European police office. URL: https://heinonline.org (дата обращения 10.05.23).
30. Europol. (2021). European Union serious and organised crime threat assessment (SOCTA). A corrupting influence: The infiltration and undermining of Europe's economy and society by organised crime. Luxembourg: Publications office of European Union URL: https://www.europol.europa.eu (дата обращения 10.05.23).
31. Federal Reserve Bank of New York (2023). Scams Involving the Federal Reserve Name. URL: https://www.newyorkfed.org/banking/frscams.html (дата обращения 10.05.23).
32. Frankel, T. (2012). The Ponzi scheme puzzle: A history and analysis of con artists and victims. New York: Oxford University Press. URL: https://scholar.google.com/scholar (дата обращения 10.05.23).
33. Ghosh S., D.L. Reilly (1994). Credit Card Fraud Detection with a Neural-Network. 27th International Conference on System Sciences. URL: https://ieeexplore.ieee.org (дата обращения 10.05.23).
34. Guardian News & Media Limited (2023). Gone in seconds: rising text message scams are draining US bank accounts. URL: https://www.theguardian.com/money/2023/apr/22/robo-texts-scams-bank-accounts (дата обращения 10.05.23).
35. Harvey, S., Kerr, J., Keeble, J., and Nicholls, C. M. (2014). Understanding victims of financial crime: a qualitative study with people affected by investment fraud. URL: https://www.fca.org.uk/publication/research/qual-study-understanding-victims-investment-fraud.pdf (дата обращения 10.05.23).
36. Heinemann, A., and Verner, D. (2006). Crime and violence in development: A literature review of Latin America and the Caribbean. World Bank policy research working paper 4041. The World Bank. URL: https://papers.ssrn.com/sol3/ (дата обращения 10.05.23).
37. Jack, J., and Ibekwe, C. C. (2018). Ponzi schemes: an analysis on coping with economic recession in Nigeria. Niger. J. Sociol. Anthropol. 16, pp. 72-90. URL: https://scholar.google.com/scholar (дата обращения 10.05.23).
38. Kadoya, Y., Khan, M. S., Narumoto, J., and Watanabe, S. (2021). Who is next? A study on victims of financial fraud in Japan. Front. Psychol. URL: https://www.ncbi.nlm (дата обращения 10.05.23).
39. Kerley, K. R., and Copes, H. (2002). Personal fraud victims and their official responses to victimization. J. Police Crim. Psychol. 17, pp. 19-35. URL: https://link.springer.com/article/10.1007/BF02802859 (дата обращения 10.05.23).
40. Langenderfer, J., and Shimp, T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: a new theory of visceral influences on persuasion. Psychol. Mark. 18, pp. 763-783. URL: https://scholar.google.com/scholar (дата обращения 10.05.23).
41. Lars Korsell (2020). Fraud in the Twenty-first Century. European Journal on Criminal Policy and Research volume 26, pp. 285-291. URL: https://link.springer.com (дата обращения 10.05.23).
42. Lea, S. E., Fischer, P., and Evans, K. M. (2009). The psychology of scams: Provoking and committing errors of judgement. London: Officer of Fair Trading. URL: https://ore.exeter.ac.uk/repository/handle/10871/20958 (дата обращения 10.05.23).
43. Lee, J., and Soberon-Ferrer, H. (1997). Consumer vulnerability to fraud: influencing factors. J. Consum. Aff. 31, pp. 70-89. URL: https://scholar.google.com/scholar (дата обращения 10.05.23).

44. Mason, K. A., and Benson, M. L. (1996). The effect of social support on fraud Victims' reporting behavior: a research note. Justice Q. 13, pp. 511-524. URL: https://www.researchgate.net/publication/240525025 (дата обращения 10.05.23).
45. Mytnyk, B.; Tkachyk, O.; Shakhovska, N.; Fedushko, S.; Syerov, Y. Application of Artificial Intelligence for Fraudulent Banking Operations Recognition. Big Data Cogn. Comput. 2023, 7, p. 93. URL: https://doi.org (дата обращения 10.05.23).
46. Nicholls J., Kuppa A., Le-Khac N.A. (2021). Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape. URL: https://www.researchgate.net/publication/356887995_Financial_Cybercrime_A_Comprehensive_Survey_of_Deep_Learning_Approaches_to_Tackle_the_Evolving_Financial_Crime_Landscape (дата обращения 10.05.23).
47. Piaw, L. L. T., Zawawi, H. B., and Bujang, Z. B. (2019). Who are the money games investors? A case study in Malaysia. Int. J. Account. 4, pp. 12-24. URL: www.ijafb.com (дата обращения 10.05.23).
48. Ramadan S., Putera A., et al, (2018). Impact of Cybercrime on Technological and Financial Developments. International Joural For Innovative Research In Multidisciplinary Field, 341-344. URL: https://www.researchgate.net/publication/329001306_Impact_of_Cybercrime_on_Technological_and_Financial_Developments (дата обращения 10.05.23).
49. Rebovich, D., and Layne, J. (2000). The national public survey on white-collar crime. Morgantown: National White-Collar Crime Center. URL: https://scholar.google.com/scholar (дата обращения 10.05.23).
50. Rossy, Q., & Ribaux, O. (2020). Orienting the development of crime analysis processes in police organisations covering the digital transformations of fraud mechanisms. European Journal on Criminal Policy and Research, 26(3). URL: https://serval.unil.ch/resource/serval:BIB_D1B9E966E9C6.P001/REF.pdf (дата обращения 10.05.23).
51. Schoepfer, A., and Piquero, N. L. (2009). Studying the correlates of fraud victimization and reporting. J Crim Just 37, pp. 209-215. URL: https://www.researchgate.net/publication/227418464_Studying_the_correlates_of_fraud_victimization_and_reporting (дата обращения 10.05.23).
52. Shadel, D., and Schweitzer-Pak, K. B. (2007). The psychology of consumer fraud. Doctoral dissertation. Tilburg: Tilburg University URL: https://research.tilburguniversity.edu/en/publications/the-psychology-of-consumer-fraud (дата обращения 10.05.23).
53. Titus, R. M., Heinzelmann, F., and Boyle, J. M. (1995). Victimization of persons by fraud. Crime Delinq. 41, pp. 54-72. URL: https://www.ojp.gov (дата обращения 10.05.23).
54. Van Wyk, J., and Benson, M. L. (1997). Fraud victimization: risky business or just bad luck? Am. J. Crim. Just. 21, pp. 163-179. URL: https://link.springer.com (дата обращения 10.05.23).
55. Waleed Hilal, S. Andrew Gadsden, John Yawney (2022). Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances. McMaster University, Canada. URL: https://dl.acm.org/doi/abs/10.1016/j.eswa.2021.116429 (дата обращения 10.05.23).
56. Whitty, M. T. (2020). Is there a scam for everyone? Psychologically profiling cyberscam victims. European Journal on Criminal Policy and Research, 26(3). URL: https://link.springer.com/article/10.1007/s10610-020-09458-z (дата обращения 10.05.23).
57. Zunzunegui, M. V., Belanger, E., Benmarhnia, T., Gobbo, M., Otero, A., Beland, F., et al. (2017). Financial fraud and health: the case of Spain. Gac. Sanit. 31, pp. 313-319. URL: https://pubmed.ncbi.nlm.nih.gov/28259392/ (дата обращения 10.05.23).

RESEARCH ARTICLE

DOI: 10.21684/2587-8484-2023-7-2-67-97 **UDC** 316.4

Financial fraud in the modern world

Elena Pavlovna Danilova[1]
Ekaterina Mikhailovna Portnyaga[2]

[1] Cand. Sci. (Soc.), Associate Professor, Department of Management and Business, Tyumen State University
e.p.danilova@utmn.ru; ORCID: 0000-0002-8254-2342

[2] Laboratory assistant researcher "Research Center", Tyumen State University
ekaterinaportnyaga@yandex.ru; ORCID: 0000-0002-0464-8838

Abstract. With the development of digital transactions and online banking, the risk of financial fraud has significantly increased. Technology has created new opportunities for fraudsters to exploit vulnerabilities in financial systems and commit crimes. Understanding the impact of technology on financial fraud in different countries is critical to developing effective strategies of its prevention and elimination, as well as to the evaluation of the effectiveness of the measures taken.

The study describes various methods used by fraudsters to manipulate digital systems, examines vulnerabilities and gaps in the current anti-fraud measures, analyzes data and trends in financial fraud, and identifies patterns in the factors making people more susceptible to fraudulent schemes.

The main goal of the research is to assess the extent of the impact of technology on financial fraud and draw conclusions about its impact on financial institutions and individuals in various geographical locations, as well as to provide an idea of the impact of technology on financial fraud in different countries and determine effective strategies for its prevention and detection.

It concludes with an insight into how the current financial fraud problems are addressed and how the importance of using advanced technology to prevent future fraud is understood. The results of the study will provide valuable insights for the organizations involved in risk management and preventive policy development in an ever-evolving technology environment.

Keywords: financial fraud; modern technologies; cybersecurity; financial literacy; cyber fraud.

Citation: Danilova E. P., Portnyaga E. M. 2023. "Financial fraud in the modern world" // Siberian Socium, vol. 7, no. 2 (24), pp. 67-97.
DOI: 10.21684/2587-8484-2023-7-2-67-97

REFERENCES

1. The Bank of Russia. Overview of transactions performed without the consent of clients of financial institutions. Accessed May 10, 2023. https://www.cbr.ru/analytics/ib/operations_survey_2022/
2. Baturin U.M., Zhodzishsky A.M. (1991). Computer crime and computer security. Accessed May 10, 2023. https://www.elibrary.ru/item.asp?id=20854436
3. Brusnikina A.E. (2015). Fraud in the financial market and ways to prevent it. Accessed May 10, 2023. https://cyberleninka.ru/article/n/moshennichestvo-na-finansovom-rynke-i-sposoby-ego-preduprezhdeniya
4. Golovinov O.N., A.V. Pogorelov (2016). Cybercrime in the modern economy: state and development trends. Accessed May 10, 2023. https://cyberleninka.ru/article/n/kiberprestupnost-v-sovremennoy-ekonomike-sostoyanie-i-tendentsii-razvitiya

5. Dadalko V.A. (2017). Methods of countering the risks of cash fraud as a tool to ensure the economic security of the organization. Accessed May 10, 2023. https://cyberleninka.ru/article/n/metody-protivodeystviya-riskam-kassovogo-moshennichestva-kak-instrument-obespecheniya-ekonomicheskoy-bezopasnosti-organizatsii
6. Maronova Z.E. (2019). Fraud in the financial market and ways to prevent it. Accessed May 10, 2023. https://cyberleninka.ru/article/n/moshennichestvo-na-finansovom-rynke-i-sposoby-ego-preduprezhdeniya-1
7. Parliamentary Newspaper (2023). Publication of the Federal Assembly of the Russian Federation. Accessed May 10, 2023. https://www.pnp.ru/social/2013/04/10/nikolay-arefev-gosudarstvo-prakticheski-zanimaetsya-otyomom-deneg-u-naseleniya.html
8. Petryakova L.A. (2020). Problems of fraud qualification in the banking sector. Accessed May 10, 2023. https://cyberleninka.ru/article/n/problemy-kvalifikatsii-moshennichestva-v-bankovskoy-sfere
9. RBK (2022). How bank fraud schemes have changed due to sanctions Accessed May 10, 2023. https://www.rbc.ru
10. RBK (2022). The Central Bank disclosed data on incidents during the transfer of funds. Accessed May 10, 2023. https://www.rbc.ru
11. Revyakin S.V. (2018). Prevention of fraud using modern electronic means of communication. Accessed May 10, 2023. https://cyberleninka.ru/article/n/profilaktika-moshennichestva-s-ispolzovaniem-sovremennyh-elektronnyh-sredstv-kommunikatsii
12. Foynitsky, I. Ya. Fraud in Russian law / I. Ya. Foynitsky. — St. Petersburg: Printing house of the Public Benefit Partnership, 1871. — 551 p. — Access mode: by subscription. Accessed May 10, 2023. https://biblioclub.ru/index.php?page=book&id=71367
13. Chikisheva N.A. (2009) Criminological characteristics of the identity of a female fraudster. Accessed May 10, 2023. https://cyberleninka.ru/article/n/kriminologicheskaya-harakteristika-lichnosti-zhenschiny-moshennitsy
14. AARP (American Association of Retired Persons) (1999). Consumer behavior, experiences and attitudes: A comparison by age groups. New Jersey: Princeton Survey Research Associates. Accessed May 10, 2023. https://www.aarp.org
15. AARP (American Association of Retired Persons) (2007). Stolen futures: An AARP Washington survey of investors and victims of investment fraud. Washington DC: AARP. Accessed May 10, 2023. https://www.aarp.org
16. Achim M.V., Borlea S.N. McGee R.W., Muresan G.M., Safta I.L., Vaidean V.L. (2020). inancial Crime: A Literature Review. Accessed May 10, 2023. https://www.researchgate.net/publication/366090442_Financial_Crime_A_Literature_Review
17. ASIC (Australian Securities & Investments Commission (2023). Accessed May 10, 2023. https://asic.gov.au/about-asic/news-centre/find-a-media-release/2023-releases/23-101mr-asic-calls-for-improved-approaches-to-scams-as-major-bank-customers-report-over-550-million-in-scam-losses/
18. Bank of America (2023). How to Avoid Scams. Accessed May 10, 2023. https://www.bankofamerica.com
19. Bolton R.J., Hand D.J. (2002). Statistical fraud detection: A review. Statistical Science, 17 (3) (2002), pp. 235-255. Accessed May 10, 2023. https://www.jstor.org/
20. Bossler A.M., Berenblum T. (2019). Introduction: new directions in cybercrime research. Accessed May 10, 2023. https://www.researchgate.net/publication/337357079_Introduction_new_directions_in_cybercrime_research
21. Burke J., Kieffer C., Mottola G. and Perez-Arce F. (2022). Can educational interventions reduce susceptibility to financial fraud? J. Econ. Behav. Organ. 198, pp. 250–266. Accessed May 10, 2023. https://scholar.google.com
22. Button M., Lewis C. and Tapley J. (2009). Fraud typologies and the victims of fraud: Literature review. London: National Fraud Authority Accessed May 10, 2023. https://researchportal.port
23. Cheng H. (2016). Financial crime in China: Developments, Sanctions, and The Systemic Spread of Corruption. New York: Palgrave Macmillan. Accessed May 10, 2023. https://scholar.google.com/scholar

24. Copes H., Kerley K. R., Mason K. A. and Van Wyk, J. (2001). Reporting behavior of fraud victims and Black's theory of law: an empirical assessment. Justice Q. 18, pp. 343-363. Accessed May 10, 2023. https://www.tandfonline.com/doi
25. Deliema M., Shadel D. and Pak K. (2020). Profiling victims of investment fraud: mindsets and risky behaviors. J. Consum. Res. 46, pp. 904-914. Accessed May 10, 2023. https://academic.oup.com
26. Dor O. (2017). Why do the Chinese continue to fall into the trap of pyramid scams? Accessed May 10, 2023. https://www.calcalist.co.il
27. Dreber A., Apicella C. L., Eisenberg D. T., Garcia J. R., Zamore R. S., Lu, J. K., et al. (2009). The 7R polymorphism in the dopamine receptor D4 gene (DRD4) is associated with financial risk taking in men. Evol. Hum. Behav. 30, pp. 85-92. Accessed May 10, 2023. https://doi.org/10.1016/j.evolhumbehav.2008.11.001
28. Eldad B. L., Liviu-George M. and Stefan-Catalin T. (2022). Financial frauds' victim profiles in developing countries. Accessed May 10, 2023. https://www.frontiersin.org
29. Europol. (2017). European Union serious and organised crime threat assessment (SOCTA). Crime in the age of technology. The Hague: European police office. Accessed May 10, 2023. https://heinonline.org
30. Europol. (2021). European Union serious and organised crime threat assessment (SOCTA). A corrupting influence: The infiltration and undermining of Europe's economy and society by organised crime. Luxembourg: Publications office of European Union Accessed May 10, 2023. https://www.europol.europa.eu
31. Federal Reserve Bank of New York (2023). Scams Involving the Federal Reserve Name. Accessed May 10, 2023. https://www.newyorkfed.org/banking/frscams.html
32. Frankel T. (2012). The Ponzi scheme puzzle: A history and analysis of con artists and victims. New York: Oxford University Press. Accessed May 10, 2023. https://scholar.google.com/scholar
33. Ghosh S., Reilly D.L. (1994). Credit Card Fraud Detection with a Neural-Network. 27th International Conference on System Sciences. Accessed May 10, 2023. https://ieeexplore.ieee.org
34. Guardian News, Media Limited (2023). Gone in seconds: rising text message scams are draining US bank accounts. Accessed May 10, 2023. https://www.theguardian.com/money/2023/apr/22/robo-texts-scams-bank-accounts
35. Harvey S., Kerr J., Keeble J. and Nicholls C. M. (2014). Understanding victims of financial crime: a qualitative study with people affected by investment fraud. Accessed May 10, 2023. https://www.fca.org.uk/publication/research/qual-study-understanding-victims-investment-fraud.pdf
36. Heinemann A, and Verner D. (2006). Crime and violence in development: A literature review of Latin America and the Caribbean. World Bank policy research working paper 4041. The World Bank. Accessed May 10, 2023. https://papers.ssrn.com/sol3/
37. Jack J. and Ibekwe C. C. (2018). Ponzi schemes: an analysis on coping with economic recession in Nigeria. Niger. J. Sociol. Anthropol. 16, pp. 72-90. Accessed May 10, 2023. https://scholar.google.com/scholar
38. Kadoya Y., Khan M. S., Narumoto J. and Watanabe, S. (2021). Who is next? A study on victims of financial fraud in Japan. Front. Psychol. Accessed May 10, 2023. https://www.ncbi.nlm
39. Kerley K. R. and Copes H. (2002). Personal fraud victims and their official responses to victimization. J. Police Crim. Psychol. 17, pp. 19-35. Accessed May 10, 2023. https://link.springer.com/article/10.1007/BF02802859
40. Langenderfer J. and Shimp T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: a new theory of visceral influences on persuasion. Psychol. Mark. 18, pp. 763-783. Accessed May 10, 2023. https://scholar.google.com/scholar
41. Lars Korsell (2020). Fraud in the Twenty-first Century. European Journal on Criminal Policy and Research volume 26, pp. 285-291. Accessed May 10, 2023. https://link.springer.com
42. Lea S. E., Fischer P., and Evans K. M. (2009). The psychology of scams: Provoking and committing errors of judgement. London: Officer of Fair Trading. Accessed May 10, 2023. https://ore.exeter.ac.uk/repository/handle/10871/20958

43. Lee J. and Soberon-Ferrer H. (1997). Consumer vulnerability to fraud: influencing factors. J. Consum. Aff. 31, pp. 70-89. Accessed May 10, 2023. https://scholar.google.com/scholar
44. Mason K. A. and Benson M. L. (1996). The effect of social support on fraud Victims' reporting behavior: a research note. Justice Q. 13, pp. 511-524. Accessed May 10, 2023. https://www.researchgate.net/publication/240525025
45. Mytnyk B., Tkachyk O., Shakhovska N., Fedushko S., Syerov Y. Application of Artificial Intelligence for Fraudulent Banking Operations Recognition. Big Data Cogn. Comput. 2023, 7, p. 93. Accessed May 10, 2023. https://doi.org
46. Nicholls J., Kuppa A., Le-Khac N.A. (2021). Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape. Accessed May 10, 2023. https://www.researchgate.net/publication/356887995_Financial_Cybercrime_A_Comprehensive_Survey_of_Deep_Learning_Approaches_to_Tackle_the_Evolving_Financial_Crime_Landscape
47. Piaw L. L. T., Zawawi H. B., and Bujang Z. B. (2019). Who are the money games investors? A case study in Malaysia. Int. J. Account. 4, pp. 12-24. Accessed May 10, 2023. www.ijafb.com
48. Ramadan S., Putera A., et al, (2018). Impact of Cybercrime on Technological and Financial Developments. International Joural For Innovative Research In Multidisciplinary Field, 341-344. Accessed May 10, 2023. https://www.researchgate.net/publication/329001306_Impact_of_Cybercrime_on_Technological_and_Financial_Developments
49. Rebovich D. and Layne, J. (2000). The national public survey on white-collar crime. Morgantown: National White-Collar Crime Center. Accessed May 10, 2023. https://scholar.google.com/scholar
50. Rossy Q., Ribaux, O. (2020). Orienting the development of crime analysis processes in police organisations covering the digital transformations of fraud mechanisms. European Journal on Criminal Policy and Research, 26(3). Accessed May 10, 2023. https://serval.unil.ch/resource/serval:BIB_D1B9E966E9C6.P001/REF.pdf
51. Schoepfer A. and Piquero, N. L. (2009). Studying the correlates of fraud victimization and reporting. J Crim Just 37, pp. 209-215. Accessed May 10, 2023.https://www.researchgate.net/publication/227418464_Studying_the_correlates_of_fraud_victimization_and_reporting
52. Shadel D. and Schweitzer-Pak, K. B. (2007). The psychology of consumer fraud. Doctoral dissertation. Tilburg: Tilburg University Accessed May 10, 2023. https://research.tilburguniversity.edu/en/publications/the-psychology-of-consumer-fraud
53. Titus R. M., Heinzelmann, F., and Boyle, J. M. (1995). Victimization of persons by fraud. Crime Delinq. 41, pp. 54-72. Accessed May 10, 2023. https://www.ojp.gov
54. Van Wyk J. and Benson, M. L. (1997). Fraud victimization: risky business or just bad luck? Am. J. Crim. Just. 21, pp. 163-179. Accessed May 10, 2023. https://link.springer.com
55. Waleed Hilal, S. Andrew Gadsden, John Yawney (2022). Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances. McMaster University, Canada. Accessed May 10, 2023. https://dl.acm.org/doi/abs/10.1016/j.eswa.2021.116429
56. Whitty M. T. (2020). Is there a scam for everyone? Psychologically profiling cyberscam victims. European Journal on Criminal Policy and Research, 26(3). Accessed May 10, 2023. https://link.springer.com/article/10.1007/s10610-020-09458-z
57. Zunzunegui M. V., Belanger, E., Benmarhnia, T., Gobbo, M., Otero, A., Beland, F., et al. (2017). Financial fraud and health: the case of Spain. Gac. Sanit. 31, pp. 313-319. Accessed May 10, 2023. https://pubmed.ncbi.nlm.nih.gov/28259392/