

Научная статья

УДК 343.988

EDN FENCHK

DOI 10.17150/2500-4255.2025.19(2).148-159



## ВЛИЯНИЕ КОГНИТИВНЫХ ИСКАЖЕНИЙ НА ПОВЕДЕНИЕ ЖЕРТВ ОНЛАЙН-МОШЕННИЧЕСТВ И ИХ УЧЕТ ПРИ РАЗРАБОТКЕ МЕР ВИКТИМОЛОГИЧЕСКОЙ ПРОФИЛАКТИКИ

Э.Л. Раднаева, Н.А. Семенова

*Бурятский государственный университет имени Доржи Банзарова, г. Улан-Удэ, Российская Федерация*

### Информация о статье

Дата поступления

10 апреля 2025 г.

Дата принятия в печать

9 июня 2025 г.

Дата онлайн-размещения

17 июня 2025 г.

### Ключевые слова

Онлайн-мошенничество; социальная инженерия; когнитивные искажения; виктимология; виктимологическая профилактика; критическое мышление; манипуляции

**Аннотация.** В условиях стремительного развития цифровой среды и усложнения схем онлайн-мошенничеств особое значение приобретает исследование психофизиологических оснований виктимного поведения. Настоящая работа посвящена выявлению роли когнитивных искажений в структуре уязвимости жертв онлайн-мошенничества и обоснованию направлений совершенствования виктимологической профилактики. Исходной методологической позицией авторов выступает признание ключевой роли перцептивных и поведенческих ошибок, совершаемых индивидом в момент принятия решения в условиях манипулятивного давления.

Анализируя как классические, так и современные исследования в области когнитивной психологии, в том числе работы Д. Канемана, а также эмпирические данные, полученные в результате обобщения конкретных кейсов мошенничества, авторы формируют систематизированный перечень наиболее значимых искажений. Устанавливается, что эмоциональные триггеры, такие, как страх, сострадание, тревожность и срочность, становятся средствами активации «первой системы» мышления, влекущей за собой утрату критической оценки ситуации. Работа обосновывает необходимость кардинального пересмотра подходов к профилактике, предлагая интеграцию знаний из когнитивистики, поведенческой экономики, социальной инженерии и юридической науки. В качестве практических выводов предложена модель адресного просвещения, включающая эмоционально-адаптированные сценарии, верифицированные поведенческие триггеры и медиамодули, воздействующие на те же механизмы восприятия, которые эксплуатируют преступники. Подчеркивается, что ключом к снижению виктимности является не только информирование, но и формирование устойчивых метакогнитивных стратегий, позволяющих субъекту противостоять манипулятивному воздействию на ранних этапах коммуникации.

Original article

## COGNITIVE BIASES INFLUENCING THE BEHAVIOR OF ONLINE FRAUD VICTIMS AND CONSIDERING THEM IN THE DEVELOPMENT OF VICTIMOLOGICAL PREVENTION MEASURES

Elvira L. Radnaeva, Natalia A. Semenova

*Buryat State University named after D. Banzarov, Ulan-Ude, Russian Federation*

### Article info

Received

2025 April 10

Accepted

2025 June 9

Available online

2025 June 17

### Keywords

Online fraud; social engineering; cognitive biases; victimology; victimological prevention; critical thinking; manipulation

**Abstract.** The rapid development of the digital environment as well as the increased complexity of online fraud schemes make the research of the psychophysiological basis of victim behavior particularly relevant. The current study is devoted to identifying the role of cognitive biases in the structure of vulnerability for online fraud victims and to showing the directions of improving the victimological practice. The methodological starting point for the authors is the recognition of the key role of mistakes of perception and behavior committed by a person at the moment of making a decision under manipulative pressure.

The authors analyze both classical and modern research of cognitive psychology, including the works of D. Kahneman, and empirical data obtained by summarizing fraud cases, and compile a systematized list of most significant biases. It is stated that emotional triggers, such as fear, compassion, anxiety and urgency, become the means of activating «system 1» thinking that eliminates the critical assessment of a situation. The authors prove the necessity of a radical reconsideration of approaches to prevention and suggest the integration of cognitive science, behavioral economy, social

engineering and legal fields of knowledge. As a practical takeaway, the authors present a model of targeted education, including emotionally-adapted scenarios, verified behavioral triggers and media-modules influencing the same perception mechanisms as those exploited by the criminals. It is stressed that the key to reducing victimity is not only the provision of information, but also the development of sustainable meta-cognitive strategies allowing a person to resist the manipulative impact at the early stages of communication.

### Введение

Исследуя способы совершения онлайн-мошенничества, невозможно не задаться вопросом о роли жертвы в механизме рассматриваемого преступного деяния. Всестороннее исследование виктимного поведения способствует разработке эффективных профилактических мер, цель которых заключается не столько в сокращении уровня онлайн-мошенничества, а в изменении системы восприятия населением информации, обладающей потенциальной криминогенной опасностью.

Целью статьи является раскрытие и объяснение механизма воздействия мошеннических схем на сознание человека, которые основаны на ошибках в восприятии информации, известных как когнитивные искажения.

Задачи статьи состоят в том, чтобы выделить общие закономерности паттернов социальной инженерии и на их основе сформулировать модель адресного виктимологического просвещения, включающая эмоционально-адаптированные сценарии, верифицированные поведенческие триггеры и медиамодули, воздействующие на те же механизмы восприятия, которые эксплуатируют преступники. В данной статье мы рассмотрим механизмы, побуждающие жертву добровольно совершать действия, требуемые преступнику, уделяя особое внимание именно когнитивным искажениям. Подробное рассмотрение механизмов действия мошеннических паттернов на поведение человека не просто дает нам понимание того, как мошенники получают желаемый результат, но, что самое главное, дает инструментарий — как использовать знания социальной инженерии для повышения рациональности и прагматизма человека при осуществлении профилактического воздействия.

### Основная часть

В процессе принятия повседневных решений человек, как правило, не склонен глубоко анализировать механизмы и когнитивные процессы, лежащие в их основе. Данную особен-

ность мышления часто используют мошенники, применяя различные виды обмана и злоупотребления доверием с целью наживы. В настоящее время интеллектуальный уровень мошенников, осуществляющих свои преступные деяния в телекоммуникационных сетях, имеет тенденцию повышаться, о чем свидетельствует развитие очень продуманных схем социальной инженерии, распознать которые зачастую представляет значительную сложность.

Когнитивными искажениями называют разнообразные систематические ошибки в мышлении человека, а также шаблонные, стереотипические отклонения, происходящие в определенных ситуациях, основой которых служат искаженные убеждения. Это могут быть ошибки в восприятии информации, анализе ситуации. Когнитивные искажения свойственны большинству людей, но в данной работе нами выдвигается гипотеза, что потенциальные жертвы онлайн-мошенничества в большей степени, чем другие люди подвержены когнитивным искажениям, которыми и пользуются киберпреступники. Вопрос, с чем это может быть связано, весьма сложен и требует качественной проработки. Основываясь на анализе научных трудов, мы можем предположить, что важнейшими условиями, позволяющими не поддаваться когнитивным искажениям мышления, лежащим в основе мошеннических манипуляций, является осведомленность индивида о механизме их действия и уровень его эмоционального интеллекта (ЭИ). Это также подтверждается исследованиями В.П. Шейнова (2019), показавшими, что низкий уровень ЭИ прямо коррелирует с повышенной виктимностью, особенно у женщин и подростков [1]. Кроме того, в противодействии мошенническим схемам большое значение имеет возможность использовать критическое мышление в ответ на манипуляционное воздействие [2]. Можно связать виктимное поведение индивида с преобладанием некоторых черт характера, таких как самоуверенность и самонадеянность, склонность к риску, суеверность, беспечность и привычка мыслить принятыми в

обществе стереотипами, что согласуется с современными мировыми трендами: в докладах Европола подчеркивается, что 84–98 % успешных кибератак происходят из-за человеческих ошибок или доверчивости [3]. Доверчивость является одним из факторов, оказывающих влияние на уровень субъективного счастья человека и, кроме того, она стоит на первом месте в ряду других виктимогенных факторов, что отражено в ежегодном "Всемирном докладе о счастье" (World Happiness Report 2024) [4].

Необходимо также отметить, что анализ 34 эмпирических исследований показал: в центре уязвимости личности — не просто «психотип», а комбинация состояния, окружения и обработки информации [5]. Учитывая изложенные аспекты и тот факт, что мошенники весьма изобретательны и мгновенно подстраиваются под изменения, мы можем с полной ответственностью заявить, что число жертв мошенничества будет расти, невзирая на технические меры профилактики, предусмотренные Федеральным законом от 1 апреля 2025 г.<sup>1</sup>.

Возвращаясь к понятию когнитивных искажений, внесем необходимые пояснения относительно природы их возникновения и функционирования. Согласно исследованиям Д. Каннемана, у человека присутствуют две системы мышления, одна из которых отвечает за быстрое (автоматическое) мышление, условно называется система 1, а вторая — за медленное (произвольное) мышление — система 2 [6]. Для преступников, занимающихся мошенничеством, важнейшим фактором является то, как жертва принимает решение (оплатить несуществующий товар или услугу, перевести деньги мошеннику, выполнить какую-либо просьбу — передать информацию и секретные данные, открывающие доступ к совершению финансовых операций). Как правило, наиболее желательным для злоумышленника будет включение у жертвы мошенничества первой системы мышления, когда человеку не требуется осознанность, и решения принимаются им очевидным образом, интуитивно, т.е. человек действует

согласно типовой ситуации. Более сложные схемы интернет-мошенничества способны воздействовать и на систему 2, используя которую для принятия решений человеку требуется осознанно контролировать происходящее, затрачивая больше энергии для концентрации внимания на определенной задаче и не отвлекаться от ее выполнения.

Как показывает практика, большинство мошеннических схем невозможно было бы реализовать без воздействия на эмоции жертвы. Именно эмоции заставляют лицо, подвергающееся воздействию злоумышленника, включать первую систему мышления в ответ на манипуляции.

Исследование, в котором приняло участие 1 027 человек в Китайской Народной Республике, выявило, что у людей с низким уровнем самоконтроля, высокой импульсивностью и высокой доверчивостью, повышены риски стать жертвой онлайн-мошенничества [7]. Такое положение вещей свидетельствует о том, что учет психологических характеристик жертвы представляется важным условием виктимологической профилактики. Главными эмоциями, отключающими рациональное мышление, являются страх, тревога, гнев, реже сострадание и любопытство. Вызывая у человека данные эмоции, преступники легко воздействуют на сознание индивида, принуждая жертву совершить те или иные действия. В комплексном обзоре исследований по податливости мошенничеству [8] рассматривается, каким образом воздействуют эмоции на обработку информации, а именно: страх и случайные негативные эмоции переводят мышление человека в автоматический режим, повышая вероятность согласия выполнить действия, предлагаемые мошенником. Нередки эпизоды, когда человек поддается воздействию вопреки тому, что он обладает информацией о подобных преступлениях и, возможно, ранее даже являлся жертвой обмана со стороны мошенников. Такое положение вещей предполагает, что при реализации профилактических мер, обращенных к потенциальным жертвам, необходимо работать с их эмоциональным состоянием и повышением уровня критического мышления. Эксперименты, проведенные исследователями из Университета Саутгемптона (University of Southampton, Великобритания) [9], показали, что люди с развитым аналитическим (система 2) мышлением лучше различают поддельные и настоящие веб-сайты. Рассмотрим, как выгля-

<sup>1</sup> О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации : Федер. закон от 1 апр. 2025 г. № 41-ФЗ // Официальный интернет-портал правовой информации. URL: <http://publication.pravo.gov.ru/document/000120250401010?index=2> (дата обращения: 06.04.2025).

дит на практике воздействие «мошеннической» социальной инженерии на жертву.

Гражданин Г., 1963 года рождения, 08.01.2023 г. на сайте «Одноклассники» получил сообщение с взломанного мошенниками аккаунта своего давнего знакомого А. о болезни его дочери В. с фотографией ребенка из онкологического центра и предложением перевести солидную сумму на лечение. Так как пользователь Г. знал, что у А. есть дочь, фото которой А. размещал у себя на странице, пользователь Г. решил, что на фото дочь А., тем более фото было размытым, а ребенок был в кислородной маске. В сообщении, кроме всего прочего, содержалась просьба оставить свой номер телефона для связи. Г. написал свой номер и отправил 3 000 руб., перейдя по ссылке и введя данные своей банковской карты в специальную форму. Через несколько часов Г. позвонил человек и, представившись сотрудником службы безопасности банка, в котором у Г. был оформлен счет, и сообщил, что на его банковском счете обнаружены подозрительные переводы, тут же поинтересовавшись, подтверждает ли он три перевода в размере 3 000, 5 000 и 15 000 руб. Г. сообщил, что переводил только 3 000 своему знакомому, сотрудник банка, попросил подробно рассказать о переводе, сказав, что уже совершает запрос в центр кибербезопасности сайта «Одноклассники». Далее мошенник сообщил Г., что страница знакомого А. была взломана, а данные карты пользователя Г. украдены, поэтому сейчас с его счета кто-то активно пытается перевести оставшуюся сумму. Далее «сотрудник банка» поинтересовался, какая сумма была в последний раз на остатке у Г., тот ответил, что примерно 57 тыс. руб. Мошенник сообщил, что, если Г. не хочет их потерять, необходимо срочно перевести их на безопасный счет. Г. согласился без тени сомнения, открыл онлайн-приложение банка и, выполняя инструкции «сотрудника банка», перевел всю оставшуюся сумму мошенникам. Прощаясь, мошенник заверил Г., что в течение трех дней вся сумма вернется на его счет в сохранности. Г. был практически уверен, что спас свои деньги. Он понял, что лишился их безвозвратно только на следующий день, когда в разговоре с приятелем рассказал о случившемся<sup>2</sup>.

<sup>2</sup> Интервью с жертвой интернет-мошенничества / Семенова Н.А. 2023. 26 сент. [неопубликованный источник]. Анонимно.

Описанный инцидент представляет собой типичный пример воздействия социальной инженерии, реализованной через переформатированное доверие и экспресс-мотиваторы. Психологические механизмы принятия решений в данной ситуации целесообразно рассматривать сквозь призму модели вероятностной обработки информации (Elaboration Likelihood Model, ELM) [10]. В рамках этой модели различаются два ключевых маршрута восприятия убеждающего сообщения: центральный, предполагающий критическую и логически выстроенную переработку информации, и периферийный, основанный на эвристиках, ассоциациях и эмоциональных реакциях.

В случае с Г. фиксация внимания произошла на поверхностных признаках достоверности сообщения — знакомое имя отправителя, фотография ребенка, внешне правдоподобная ситуация и срочный характер просьбы. Подобные элементы запускают механизмы автоматического реагирования, что было зафиксировано во множестве эмпирических исследований, таких как Vishwanath, 2015 [11], Harrison et al., 2016 [12]. Наличие эмоционального триггера в виде онкологического заболевания ребенка значительно снижает вероятность аналитической проверки сообщения, что характерно для периферийного маршрута обработки. В работах Д. Канемана такое поведение человека соответствует первой — автоматической системе мышления. Таким образом, анализ поведения респондента указывает на снижение когнитивного контроля в условиях стрессогенной информационной атаки. Это позволяет утверждать, что повышать устойчивость к мошенническим воздействиям следует через развитие навыков метакогнитивной саморегуляции, обучение узнаванию структур фишинга и переводу восприятия в режим центральной переработки, особенно в условиях социальной перегрузки или эмоционального давления. Об этом неоднократно заявляли в своих работах также российские ученые [13].

При более детальном рассмотрении механизма мошеннических действий и методов социальной инженерии в вышеприведенном случае можно говорить о том, что эмоция сострадания мотивировала Г. перевести 3 000 руб. на счет мошенников. То, что этот пользователь откликнулся на манипуляцию эмоцией сострадания, говорит о наличии у него аффективно-когнитивной структуры, которую можно определить как отклик на конкретный образ, в данном случае на больного



ребенка. Аффективно-когнитивная структура может проявляться как ценность, цель или идеал, а комплекс таких структур может стать основой мировоззрения или идеологии [6]. Воздействуя на правильно определенную аффективно-когнитивную структуру, злоумышленник легко понуждает жертву совершать необходимые ему действия. После того как мошенники завладели номером телефона Г., они сообщили ему о переводах с его карты, один из которых он действительно совершал, а два другие нет. Восприняв знакомую информацию, Г. без сомнения поверил, что с ним разговаривает сотрудник службы безопасности банка. В этом случае мошенники воздействовали на Г. с помощью эмоции страха (потерять деньги). Эмоция страха очень сильна, она отключила рациональное мышление, поэтому Г. выполнил инструкции мошенников, переводя им на счет остаток денежных средств со своей банковской карты.

Исходя из приведенного примера, мы имеем возможность предположить, что профилактика таких манипуляций должна быть направлена не просто на информирование граждан о методах обмана мошенниками, а прежде всего на объяснение того, как и почему данная схема работает. В связи с этим, по нашему мнению, профилактическую информацию неопределенному числу людей целесообразно представлять в виде научно-популярных статей под броскими заголовками, например «Почему порядочные люди чаще становятся жертвами мошенников?». Данный заголовок с высокой вероятностью привлечет внимание, поскольку в его формулировке содержится когнитивное искажение, которое влияет на восприятие большинства людей, считающих себя порядочными гражданами и, естественно, не желающих стать жертвами мошенничества. Также профилактическую информацию можно разместить в виде короткого видеоролика продолжительностью не более полутора минут с сюжетом, в котором герой подвергается воздействию мошенников. Подобные видеоролики, выпущенные в рамках европейской инициативы *Cyber Scams Awareness*, зарекомендовали себя как эффективный инструмент в повышении настороженности пользователей к фишинговым письмам [14]. Кроме представления самой мошеннической схемы, в виктимологические материалы необходимо включать информацию о том, как безопасно помогать нуждающимся, как этично реагировать на просьбы о помощи в соци-

альных сетях или по телефону. Стоит отметить, что мошенничество в сети Интернет отличается более продуманными и хитрыми схемами, нежели мошенничество с использованием только телефонов. В интернете есть необходимость предварительной «обработки» жертвы, внедрения в ее сознание альтернативной реальности, необходимой для реализации преступного замысла. Для реализации преступных намерений жертве может быть отправлено письмо на электронный адрес или сообщение в мессенджер, в котором сообщается, например, о попытках взлома, блокировки аккаунта в социальной сети, учетной записи портала «Госуслуги», кабинета налогоплательщика (даже если его нет) или какого-то другого важного ресурса, в зависимости от имеющейся у преступника информации о потенциальной жертве. В этом же сообщении предлагается узнать подробности, пройдя по «ссылке» либо «для разблокировки перейдите в личный кабинет», при этом часто ссылка маскируется кнопкой «перейти». Таким образом, мошенники рассчитывают на некритическое восприятие информации. Проходя по ссылке, пользователь попадает на сайт, внешне не отличающийся от того, на котором расположена его страница или личный кабинет (госуслуги, сайт банка и т.д.), где пользователю предлагается специальное поле для введения пароля и логина. Для усиления чувства беспокойства на данном сайте может быть показан таймер, отсчитывающий секунды для совершения операции ввода данных. Данная деталь используется многими настоящими сайтами при оплате услуг, поэтому особого подозрения не вызывает. После того, как данные доступа введены в специальные поля, они попадают в руки мошенников. Но чтобы жертва не опомнилась, ей могут быть предложены несколько вариантов дальнейших действий, например, может всплыть окно с надписью «сайт временно не работает», «войдите через приложение» или дана фальшивая ссылка на приложение. Жертва снова переходит по ссылке, вводит логин и пароль, далее мошеннический сайт может имитировать загрузку или повторить просьбу подтвердить какие-либо данные. Таким образом, мошенники затягивают время, которое используют для доступа в личный кабинет жертвы либо на ее страницу, в зависимости от целей. Здесь злоумышленники ориентируются уже не столько на эмоцию страха, сколько на эмоцию удивления и стремление потенциальной жертвы разобраться в ситуации.

Подчеркнем, мошенники все чаще стали использовать методы, которые вполне успешно работают со второй системой мышления. Рассмотрим подобный случай. В 2022 г. появился новый вид мошенничества. Злоумышленник под видом рекрутера, менеджера по персоналу предлагает жертве трудоустроиться на высокооплачиваемую работу, общается с клиентом несколько дней, присылает разные анкеты с предложением их заполнить, может устроить собеседование по видеоконференции. Затем сообщает, что на должность есть еще несколько кандидатов, и дополнительные баллы получит тот, кто имеет сертификат центра корпоративного обучения. Чтобы его получить, необходимо пройти обучающие курсы в течение двух недель. Естественно, курсы жертва пройти не успевает, на что мошенник предлагает оплатить курсы, которые уже подходят к концу, а он договорится о выдаче сертификата. После чего направляет клиента на специально созданный сайт «корпоративного обучения», через который клиент добровольно оплачивает эти курсы. После чего ему выдается сертификат, а мошенник либо пропадает, либо говорит, что, увы, клиент опоздал, но будет включен в кадровый резерв. В данном случае мошенники заставляют человека сконцентрироваться на одной задаче, но не дают ему времени для анализа ситуации, включая его первую систему мышления. Именно поэтому данный метод применим к людям с высоким уровнем интеллекта. И даже на этом примере мы видим, что для получения результата мошенникам нужно создать такие условия, чтобы жертва опиралась на систему мышления 1 (автоматическую).

Давайте подробнее разберем на этом примере действие когнитивных искажений на психику жертвы. Можно предположить, что в данном контексте работает эффект обратной связи (англ. *backfireeffect*) — это когнитивное искажение, при котором человек начинает еще сильнее верить в дезинформацию после того, как ему представлена корректирующая информация [15]. Люди склонны считать правдой ту информацию, которая им знакома; в данном случае проявляется тип эффекта обратной связи — «ложная правда». Результаты исследования показывают, что феномен ложной правды проявляется не только в отношении фактических утверждений, но также и в восприятии субъективных мнений. Повторяющиеся суждения, даже те, которые изначально не совпадали с убежде-

ниями человека, начинают казаться ему более правдоподобными. Это подчеркивает важность овладения навыками критического осмысления информации и осознания того, что сама по себе повторяемость высказывания способна создавать иллюзию его достоверности, независимо от его реальной истинности [16]. Большую роль играет и то обстоятельство, что по своей природе люди более доверчивы к открытым, экстравертированным собеседникам или системам, исходящая от них информация не встречает выраженного сопротивления и мало подвергается критике, кроме того, обратная связь повышает вовлеченность в процессе [17]. В данном паттерне мошенничества когнитивное искажение изменяет поведение человека именно по той причине, что правильно подобрано место и время его использования: дезинформация подается дозированно, и это постоянно подкрепляет уверенность жертвы в правильности своих действий. Однако, по мнению некоторых ученых, эффект обратной связи, именно тип «*worldviewbackfireeffect*», встречается не так часто [18], что ставит под сомнение его устойчивость как феномена. Тем не менее исследования в настоящий момент нельзя назвать окончательными. Необходимо учитывать, что эффект «ложной правды» подавляется, если человек знает, что информация ложная [15]. Именно этот аспект можно успешно использовать в криминологической профилактике, донося до как можно большего числа граждан информацию о мошеннических схемах, отмечая неправдоподобность данных манипуляторных действий.

Данный вид мошенничества целиком и полностью построен на обмене информацией между злоумышленником и жертвой. Мошенник обрабатывает человека, постоянно держит его в поле воздействия, используя при этом и другие когнитивные искажения, присущие индивиду. Здесь мы отчетливо можем проследить, как работает когнитивное искажение, называемое «иллюзорное превосходство» или эффект «лучше среднего» [19]. Речь идет о типичной когнитивной ошибке, когда человек воспринимает собственные качества и навыки как превосходящие таковые у других. В силу предвзятости восприятия потенциальная жертва не заостряет своего внимания на том, что предлагаемая должность подозрительно заманчивая, а заработная плата подчас намного выше средней в данной профессии. В завершающем этапе преступного деяния, когда злоумышленникам необходимо

получить от «соискателя» деньги, у последнего автоматически возникает «эффект оправдания усилий» [20], что способствует совершению им ложной покупки сертификата. Вместо покупки сертификата может быть дача взятки, внесение залога и прочие действия по передаче денежных средств субъекту мошенничества. В серии экспериментов, проведенных в Университете Корнелла (Cornell University) и Университете Колорадо в Боулдере (University of Colorado Boulder), было показано, что объекты, которые, как считалось, потребовали больше усилий для создания, оценивались как более качественные [21]. Говоря об эффекте оправдания усилий, в нашем случае мы имеем в виду, что человеку нелегко отказаться от идеи, на которую он затратил время и усилия по поиску работы, включающие в себя заполнение анкеты, собеседование, разговоры с предполагаемым работодателем и тому подобные действия, приближающие получение «заветной» должности. Критика со стороны в данном случае будет восприниматься весьма болезненно, так как жертва, благодаря манипуляциям, уже поверила в себя, в свою состоятельность и успех, и страстно желает подтверждения своих иллюзий в получении желаемого. Эффект оправдания усилий также неплохо работает в различных ставках на спорт. Однако в этих ситуациях наиболее заметно реализуется оптимистическое искажение, которое состоит в том, что люди склонны переоценивать вероятность положительных событий и недооценивать вероятность отрицательных [22].

Оптимистическое искажение — сложное явление, которое снижает тревогу и способствует формированию защитного поведения [23], подталкивая потенциальную жертву к участию в мошеннических проектах, таких как вложение денег в криптовалюту, инвестирование в ложные проекты, покупка несуществующих акций. Оптимистическое искажение работает как механизм между эмоциональной обработкой информации и поведенческими выборами [24]. В то же время оно серьезно ослабевает, если угроза становится лично значимой [25], например, когда человек сталкивается с тем, что в его окружении кто-то пострадал от мошенников или человек сам получил негативный опыт. Данный аспект представляется важным для использования в профилактических целях: регулярная информация о жертвах мошенничества, корректно и правильно доносямая до целевых аудиторий, будет способствовать повышению

бдительности. При реализации образовательных программ по виктимологической профилактике важно, чтобы они включали модули по поведенческим искажениям и эмоциональному самоконтролю. Следует иметь в виду, что ощущение личного контроля над ситуацией может усиливать оптимистическое искажение [26].

Еще одним очень распространенным искажением, которое часто используют онлайн-мошенники, является склонность к подтверждению своей точки зрения, или предвзятость подтверждения [27] — это когнитивный процесс, при котором индивиды демонстрируют склонность к выборочному поиску информации, направленному на подтверждение уже сформированных у них убеждений или точек зрения. При воплощении сценария со звонком из службы безопасности банка, отдела полиции или других правоохранительных структур, жертва уже внутренне подозревает, что с ее счетом может быть что-то не так (например, недавно заходила в онлайн-банк или слышала о взломах). То есть информация воспринимается не критично, а через фильтр уже существующего ожидания. Все действия мошенника (голос уверенный, называет банк, знает имя клиента) становятся для жертвы доказательствами достоверности, возникающие сомнения жертва интерпретирует как свою тревожность, а не как сигнал опасности. Согласно Р.С. Никерсону [27], предвзятость подтверждения — это не просто ошибка мышления, а естественный механизм поддержания когнитивного комфорта. Именно поэтому жертвы телефонного мошенничества часто доверяют даже абсурдным сообщениям, так как те встраиваются в уже существующий тревожный или эмоциональный контекст. Жертва интернет-мошенничества, получившая подозрительное электронное письмо, может изначально поверить в его подлинность, так как оно содержит информацию, которая соответствует ее ожиданиям, например, предложение о выигранной лотерее. Но, относясь легкомысленно даже к явным признакам мошенничества, таким как орфографические ошибки, подозрительные ссылки, человек начинает искать подтверждение того, что письмо подлинное. Например, он может припоминать о своем недавнем участии в лотерее, выигрыше в онлайн-казино или подтвердить, что пользуется сайтом, указанным в письме. В результате жертва укореняется в своем предвзятом мнении и может проигнорировать признаки мошенничества, что, соот-

ответственно, приводит к совершению ошибок, таких как переход по ссылке, предоставление конфиденциальной информации (кода из SMS), перевод денег. Мошенники часто пользуются тем, что, получив тревожное сообщение, например о блокировке карты, потенциальная жертва не задает критических вопросов, а скорее проверяет в интернете лишь те сведения, которые укладываются в заданную тревожную рамку. Вместо запроса «признаки мошенничества» набирает «почему банк блокирует карту без предупреждения», тем самым подкрепляя внутреннюю убежденность в достоверности угрозы. Современные исследования, в частности работа Suzuki и Yamamoto (2021) [28], показывают, что при взаимодействии с поисковыми системами пользователи склонны выбирать те результаты, которые соответствуют их исходным представлениям. В этой связи мы предполагаем, что при разработке антифрод-интерфейсов должны быть использованы технологии, которые нарушают паттерны подтверждения. А вот сайты — подделки под известные банки работают, благодаря искажению «предпочтение знакомого». Исследование Р. Борнштейна и П. Д'Агостино [29] посвящено объяснению эффекта простой экспозиции (*mere exposure effect*) — когнитивного искажения, при котором повторное предъявление одного и того же стимула повышает его привлекательность. Авторы предлагают рассматривать этот эффект не как автоматическое усиление положительного отношения, а как следствие, снижение субъективной неопределенности по отношению к стимулу. Этот аспект особенно важен в контексте виктимного поведения в интернете: люди чаще доверяют сообщениям, сайтам или стилям общения, которые уже встречались им ранее, просто потому что они знакомы и воспринимаются как менее угрожающие. Видя знакомый образ, логотип и даже узнавая стиль письма, люди не обращают внимания на адрес в строке браузера и спокойно оплачивают товары, услуги, совершают денежные переводы мошенникам.

### Заключение

В данной работе мы рассмотрели далеко не все когнитивные искажения, лежащие в основе мошеннических схем, однако уже этого достаточно для того, чтобы сделать определенные выводы относительно направлений виктимологической профилактики преступности в телекоммуникационных сетях. Анализ механизмов

социальной инженерии и когнитивных искажений, используемых мошенниками, показывает, что жертва играет ключевую роль в процессе мошенничества. А важнейшими детерминантами виктимизации в данном случае выступают субъективные виктимогенные факторы, т.е. индивидуальные личностные особенности самого потерпевшего [30]. По мнению профессора А.Л. Репецкой, эффективное противодействие данному виду мошенничества может быть оказано при использовании средств именно виктимологической профилактики [31]. Понимание того, как эмоциональные и когнитивные факторы влияют на принятие решений, позволяет нам не только раскрыть схемы обмана, но и разработать более эффективные виктимологические меры.

Важно не просто информировать граждан о методах мошенничества, но и изменить их восприятие и поведение через целенаправленное просвещение, в том числе научно-популярные материалы и короткие видеоролики, которые наглядно демонстрируют механизмы манипуляций и способы защиты от них. Кроме того, профилактика мошенничества должна быть основана на комплексном подходе, включающем использование знаний виктимологии, социальной инженерии, когнитивистики и психологии принятия решений. Это позволит создать более устойчивую к манипуляциям среду, в которой потенциальные жертвы будут способны защищать себя и свои финансовые ресурсы от злоумышленников.

При разработке программ профилактики онлайн-мошенничества стоит учитывать действие когнитивных искажений, например эффекта простой экспозиции, так как это не только важный когнитивный механизм, но и фундаментальный путь к бессознательному влиянию [32], поэтому его необходимо использовать в разработке антифрод-систем и просветительских материалов.

Подводя итог, с большой долей вероятности можно сделать вывод о том, что жертвы онлайн-мошенничества при принятии решений чаще действуют «на автомате», опираясь на систему мышления 1, иногда не учитывая ни свой личный опыт общения с мошенниками, ни виктимологическую информацию, имеющуюся в достаточном количестве. Поэтому ответом на важнейший вопрос, которым часто задаются правоохранители: «Почему профилактическая информация в виде листовок, баннеров и предупреждений на сайтах и в приложениях финан-



совых и кредитных организаций не работает?», будет тот факт, что когнитивные искажения по своему воздействию на сознание гораздо сильнее, чем какая-либо информация, на которую у человека не поступало запроса. Такая профилактическая информация воспринимается как информационный шум. Кроме того, под воздействием социальной инженерии, особенно при принятии решений о переводе денежных средств, человек по привычке, экономя ресурсы, не включает энергозатратную систему мышления 2, которая позволила бы ему разобраться в ситуации.

Для удобства восприятия информации по профилактическим мерам представляем таблицу.

Учитывая данные факты, можно предположить, что профилактическая информация тре-

бует доработки в плане объяснения людям их способа мышления и особенностей принятия решений, это представляется трудоемким, но очень действенным. Основным фактором эффективности виктимологического просвещения должна быть адресность информации, т.е. целевая аудитория, которую можно распределить на группы, например: школьники, соискатели вакансий, работники мелких предприятий, индивидуальные предприниматели, пенсионеры, посетители сайтов знакомств и др. Профилактическая информация должна включать в себя обучающий компонент, направленный на то, чтобы люди без усилий автоматически идентифицировали мошеннические уловки, отказывались от контакта с субъектом мошенничества на самых ранних стадиях коммуникации. В связи с

### Механизмы виктимизации и профилактические меры Mechanisms of victimization and prevention measures

Механизм / Mechanism	Суть / Essence	Проявление в мошенничестве / Manifestation in fraud	Профилактические меры / Prevention measures
Предвзятость подтверждения / Confirmation bias	Склонность искать и интерпретировать информацию, подтверждающую существующие убеждения	Жертва игнорирует признаки обмана, потому что сообщение кажется ей правдоподобным и знакомым	Повышение уровня эмоционального интеллекта. Обучение навыкам критического мышления, включение в тренинги модулей по проверке альтернативных точек зрения, формирование привычки задавать уточняющие вопросы
Эффект простой экспозиции / Simple exposition effect	Повторяемость стимула делает его более привлекательным или вызывающим доверие	Частое упоминание бренда/банка в сообщениях вызывает ложное ощущение легитимности	Разработка антифрод-обучающих материалов, в которых разъясняется, что узнаваемость ≠ достоверность; примеры подделок с визуальной имитацией официальных ресурсов
Оптимистическое искажение / Optimistic bias	Переоценка вероятности положительных исходов и недооценка риска	Жертва считает, что с ней «такого не произойдет» и не проверяет информацию	Просветительские кампании с акцентом на реальные кейсы жертв, формирование реалистичной оценки вероятностей угроз через цифровое просвещение
Иллюзия контроля / Illusion of control	Человек переоценивает степень своего влияния на исход событий	Пользователь уверен, что контролирует ситуацию, и следует инструкциям мошенника	Обучение распознаванию признаков манипуляции и ложно создаваемого чувства контроля. Модули по оценке доверенности источника информации
Ощущение срочности / Feeling of urgency	Эмоциональный стресс снижает способность к критическому мышлению	Сообщения типа «осталось 5 минут» вынуждают действовать импульсивно	Создание антифрод-интерфейсов, которые вводят обязательную задержку или паузу, использование push-уведомлений с напоминанием «подумай еще раз перед действием»
Когнитивная нагрузка / Cognitive load	Перегрузка информацией снижает способность анализировать содержание	Жертва в состоянии усталости или тревожности не распознает подвох	Минимализм и понятность интерфейсов, обучение методам саморегуляции и цифровой гигиене, особенно для пожилых и уязвимых групп

этим предполагается использование когнитивных искажений и психологических механизмов, на которых основываются мошеннические схемы, в целях создания методик, направленных на противодействие манипуляциям. Это по-

зволит разработать стратегии, направленные на повышение уровня критического мышления и осознанности у потенциальных жертв, что, в свою очередь, способствует снижению их уязвимости к мошенническим воздействиям.

### СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Шейнов В.П. Взаимосвязи виктимизации и эмоционального интеллекта: половозрастные особенности / DOI 10.22363/2313-1683-2019-16-3-377-392. — EDN FTDKXN // Вестник Российского университета дружбы народов. Сер.: Психология и педагогика. — 2019. — Т. 16, № 3. — С. 377–392.
2. Филатов А. Когнитивные искажения и иллюзии мозга / А. Филатов. — Москва : Перо, 2020. — 348 с.
3. Cybercriminal Exploitation of Cognitive Biases: A Brain Capital Perspective / I. MacRae, R. Ojha, E. Smith [et al.] // *Psychiatric Times*. — 2022. — 27 July. — URL: <https://www.psychiatrictimes.com/view/cybercriminal-exploitation-of-cognitive-biases-a-brain-capital-perspective>.
4. World Happiness Report 2024 / eds. J.F. Helliwell, R. Layard, J.D. Sachs [et al.]. — Oxford : Wellbeing Research Centre, 2024. — URL: <https://worldhappiness.report/ed/2024/>.
5. Norris G. The Psychology of Internet Fraud Victimization: a Systematic Review / G. Norris, A. Brookes, D. Dowell. — DOI 10.1007/s11896-019-09334-5 // *Journal of Police and Criminal Psychology*. — 2019. — Vol. 34. — P. 231–245.
6. Канеман Д. Думай медленно... решай быстро / Д. Канеман. — Москва : АСТ, 2023. — 903 с.
7. Zhang Z. The role of Social-Psychological Factors of Victimity on Victimization of Online Fraud in China / Z. Zhang, Z. Ye. — DOI 10.3389/fpsyg.2022.1035189 // *Frontiers in Psychology*. — 2023. — Vol. 13. — URL: <https://www.frontiersin.org/articles/10.3389/fpsyg.2022.1035189/full>.
8. Mental States: A Key Point in Scam Compliance and Warning Compliance in Real Life / X. Wen, L. Xu, J. Wang [et al.]. — DOI 10.3390/ijerph19148294 // *International Journal of Environmental Research and Public Health*. — 2022. — Vol. 19, no. 14. — URL: <https://www.mdpi.com/1660-4601/19/14/8294>.
9. Analytical Reasoning Reduces Internet Fraud Susceptibility / N.J. Kelley, A.L. Hurley-Wallace, K.L. Warner, Y. Hanoch. — DOI 10.1016/j.chb.2022.107648 // *Computers in Human Behavior*. — 2023. — Vol. 140. URL: <https://www.sciencedirect.com/science/article/pii/S074756322200468X>.
10. Petty R.E. The Elaboration Likelihood Model of Persuasion / R.E. Petty, J.T. Cacioppo. — DOI 10.1016/S0065-2601(08)60214-2 // *Advances in Experimental Social Psychology*. — 1986. — Vol. 19. — P. 123–205.
11. Vishwanath A. Examining the Distinct Antecedents of E-Mail Habits and its Influence on the Outcomes of a Phishing Attack / A. Vishwanath. — DOI 10.1111/jcc4.12127 // *Journal of Computer-Mediated Communication*. — 2015. — Vol. 20, no. 5. — P. 570–584.
12. Harrison B. Individual Processing of Phishing Emails: How Attention and Elaboration Protect Against Phishing / B. Harrison, E. Svetieva, A. Vishwanath. — DOI 10.1108/OIR-10-2015-0332 // *Online Information Review*. — 2016. — Vol. 40, no. 2. — P. 265–281.
13. Чуб И.С. Мошенничество в сети Интернет: способы совершения и виктимологическая профилактика / И.С. Чуб. — EDN ZESIFE // Вестник Краснодарского университета МВД России. — 2024. — № 1 (63). — С. 39–42.
14. Siddiqi M.A. A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures / M.A. Siddiqi, W. Pak, M.A. Siddiqi // *Applied Sciences*. — 2022. — Vol. 12, no. 12. — P. 6042.
15. Swire-Thompson B. Searching for the Backfire Effect: Measurement and Design Considerations / B. Swire-Thompson, J. DeGutis, D. Lazer // *Journal of Applied Research in Memory and Cognition*. — 2020. — Vol. 9, no. 3. — P. 286–299.
16. Knowledge Does not Protect against Illusory Truth / L.K. Fazio, N.M. Brashier, B.K. Payne, E.J. Marsh. — DOI 10.1037/xge0000098 // *Journal of Experimental Psychology: General*. — 2015. — Vol. 144, no. 5. — P. 993–1002.
17. Изард К.Э. Психология эмоций / К.Э. Изард. — Санкт-Петербург : Питер, 2008. — 460 с.
18. Wood T. The Elusive Backfire Effect: Mass Attitudes' Steadfast Factual Adherence / T. Wood, E. Porter. — DOI 10.1007/s11109-018-9443-y // *Political Behavior*. — 2019. — Vol. 41, no. 1. — P. 135–163.
19. Svenson O. Are We All Less Risky and More Skillful Than our Fellow Drivers? / O. Svenson. — DOI 10.1016/0001-6918(81)90005-6 // *Acta Psychologica*. — 1981. — Vol. 47, no. 2. — P. 143–148.
20. Aronson E. The Effect of Severity of Initiation on Liking for a Group / E. Aronson, J. Mills. — DOI 10.1037/h0047195 // *Journal of Abnormal and Social Psychology*. — 1959. — Vol. 59, no. 2. — P. 177–181.
21. The Effort Heuristic / J. Kruger, D. Wirtz, L. Van Boven, T.W. Altermatt. — DOI 10.1016/S0022-1031(03)00065-9 // *Journal of Experimental Social Psychology*. — 2004. — Vol. 40, no. 1. — P. 91–98.
22. Sharot T. The Optimism Bias / T. Sharot. — DOI 10.1016/j.cub.2011.10.030 // *Current Biology*. — 2011. — Vol. 21, no. 23. — P. R941–R945.
23. Lyu D. Optimism Bias, Judgment of Severity, and Behavioral Change During Two Stages of the Pandemics in China / D. Lyu, F. Jia, X. Gai. — DOI 10.1038/s41598-024-84057-0 // *Scientific Reports*. — 2025. — Vol. 15. — URL: <https://doi.org/10.1038/s41598-024-84057-0>.
24. Mediating Role of Optimism Bias and Risk Perception Between Emotional Intelligence and Decision-Making: A Serial Mediation Model / C. Chen, M. Ishfaq, F. Ashraf [et al.]. — DOI 10.3389/fpsyg.2022.914649 // *Frontiers in Psychology*. — 2022. — Vol. 13. — URL: <https://doi.org/10.3389/fpsyg.2022.914649>.
25. Helweg-Larsen M. Do Moderators of the Optimistic Bias Affect Personal or Target Risk Estimates? A Review of the Literature / M. Helweg-Larsen, J.A. Shepperd. — DOI 10.1207/S15327957PSPR0501\_5 // *Personality and Social Psychology Review*. — 2001. — Vol. 5, no. 1. — P. 74–95.


26. Blanco F. Interaction between the Illusion of Control and the Personal Involvement of the Participants / F. Blanco, H. Matute, M.A. Vadillo. — DOI 10.1016/j.concog.2011.12.001 // *Consciousness and Cognition*. — 2012. — Vol. 21, no. 1. — P. 423–432.
27. Nickerson R.S. Confirmation Bias: A Ubiquitous Phenomenon in Many Guises / R.S. Nickerson. — DOI 10.1037/1089-2680.2.2.175 // *Review of General Psychology*. — 1998. — Vol. 2, no. 2. — P. 175–220.
28. Suzuki S. Characterizing the Influence of Confirmation Bias on Web Search Behavior / S. Suzuki, Y. Yamamoto. — DOI 10.3389/fpsyg.2021.771948 // *Frontiers in Psychology*. — 2021. — Vol. 12. — URL: <https://www.frontiersin.org/articles/10.3389/fpsyg.2021.771948/full>.
29. Bornstein R.F. The Mere Exposure Effect: An Uncertainty Reduction Explanation Revisited / R.F. Bornstein, P.R. D'Agostino. — DOI 10.1177/0146167292181015 // *Personality and Social Psychology Bulletin*. — 1992. — Vol. 18, no. 1. — P. 130–139.
30. Заварыкин И.Н. Профилактика преступлений: виктимологический аспект / И.Н. Заварыкин. — Барнаул : Барнаул. юрид. ин-т МВД России, 2021. — 88 с. — EDN RPSVQQ.
31. Репецкая А.Л. Криминологический анализ современного состояния мошенничеств в банковской сфере России / А.Л. Репецкая, Л.А. Петрякова. — DOI 10.24147/1990-5173.2022.19(1).62-72. — EDN PSPQXA // *Вестник Омского университета. Серия: Право*. — 2022. — Т. 19, № 1. — С. 62–72.
32. Zajonc R.B. Mere Exposure: A Gateway to the Subliminal / R.B. Zajonc. — DOI 10.1111/1467-8721.00154 // *Current Directions in Psychological Science*. — 2001. — Vol. 10, no. 6. — P. 224–228.


## REFERENCES

1. Sheinov V.P. Relation Between Victimization and Emotional Intelligence: Gender and Age Features. *Vestnik Rossiiskogo universiteta družby narodov. Seriya: Psikhologiya i pedagogika = RUDN Journal of Psychology and Pedagogy*, 2019, vol. 16, no. 3, pp. 377–392. (In Russian). EDN: FTDKXN. DOI: 10.22363/2313-1683-2019-16-3-377-392.
2. Filatov A. *Cognitive Distortions and Brain Illusions*. Moscow, Pero Publ., 2020. 348 p.
3. MacRae I., Ojha R., Smith E., Krawczyk D., Berk M., Eyre H.A. Cybercriminal Exploitation of Cognitive Biases: A Brain Capital Perspective. *Psychiatric Times*, 2022, 27 July. URL: <https://www.psychiatrictimes.com/view/cybercriminal-exploitation-of-cognitive-biases-a-brain-capital-perspective>.
4. Helliwell J.F., Layard R., Sachs J.D., De Neve J.-E., Aknin L.B., Wang S. (eds.). *World Happiness Report 2024*. Oxford, Wellbeing Research Centre, 2024. URL: <https://worldhappiness.report/ed/2024>.
5. Norris G., Brookes A., Dowell D. The Psychology of Internet Fraud Victimization: a Systematic Review. *Journal of Police and Criminal Psychology*, 2019, vol. 34, pp. 231–245. DOI: 10.1007/s11896-019-09334-5.
6. Kahneman D. *Thinking, Fast and Slow*. New York, 2011. 542 p. (Russ. ed.: Kaneman D. *Think Slowly... Decide Quickly*. Moscow, AST Publ., 2023. 903 p.).
7. Zhang Z., Ye Z. The Role of Social-Psychological Factors of Victimity on Victimization of Online Fraud in China. *Frontiers in Psychology*, 2023, vol. 13. URL: <https://www.frontiersin.org/articles/10.3389/fpsyg.2022.1035189/full>.
8. Wen X., Xu L., Wang J. [et al]. Mental States: A Key Point in Scam Compliance and Warning Compliance in Real Life. *International Journal of Environmental Research and Public Health*, 2022, vol. 19, no. 14. URL: <https://www.mdpi.com/1660-4601/19/14/8294>.
9. Kelley N. J., Hurley-Wallace A. L., Warner K. L., Hanoch Y. Analytical Reasoning Reduces Internet Fraud Susceptibility. *Computers in Human Behavior*, 2023, vol. 140. URL: <https://www.sciencedirect.com/science/article/pii/S074756322200468X>.
10. Petty R.E., Cacioppo J.T. The Elaboration Likelihood Model of Persuasion. *Advances in Experimental Social Psychology*, 1986, vol. 19, pp. 123–205. DOI: 10.1016/S0065-2601(08)60214-2.
11. Vishwanath A. Examining the Distinct Antecedents of E-Mail Habits and its Influence on the Outcomes of a Phishing Attack. *Journal of Computer-Mediated Communication*, 2015, vol. 20, no. 5, pp. 570–584. DOI: 10.1111/jcc4.12127.
12. Harrison B., Svetieva E., Vishwanath A. Individual Processing of Phishing Emails: How Attention and Elaboration Protect Against Phishing. *Online Information Review*, 2016, vol. 40, no. 2, pp. 265–281. DOI: 10.1108/OIR-10-2015-0332.
13. Chub I.S. Internet Fraud: Methods of Committing and Victimological Prevention. *Vestnik Krasnodarskogo universiteta MVD Rossii = Bulletin of the Krasnodar University of Ministry of Internal Affairs of Russia Bulletin*, 2024, no. 1, pp. 39–42. (In Russian). EDN: ZESIPE.
14. Siddiqi M.A., Pak W., Siddiqi M.A. A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Applied Sciences*, 2022, vol. 12, no. 12, pp. 6042.
15. Swire-Thompson B., DeGutis J., Lazer D. Searching for the Backfire Effect: Measurement and Design Considerations. *Journal of Applied Research in Memory and Cognition*, 2020, vol. 9, no. 3, pp. 286–299.
16. Fazio L.K., Brashier N.M., Payne B.K., Marsh E.J. Knowledge does not Protect against Illusory Truth. *Journal of Experimental Psychology: General*, 2015, vol. 144, no. 5, pp. 993–1002. DOI: 10.1037/xge0000098.
17. Izard K.Eh. *The Psychology of Emotions*. New York, Plenum Press, 1991. 451 p. (Russ. ed.: Izard K.Eh. *The Psychology of Emotions*. Saint Petersburg, Piter Publ., 2008. 460 p.).
18. Wood T., Porter E. The Elusive Backfire Effect: Mass Attitudes' Steadfast Factual Adherence. *Political Behavior*, 2019, vol. 41, no. 1, pp. 135–163. DOI: 10.1007/s11109-018-9443-y.
19. Svenson O. Are We All Less Risky and More Skillful than our Fellow Drivers? *Acta Psychologica*, 1981, vol. 47, no. 2, pp. 143–148. DOI: 10.1016/0001-6918(81)90005-6.
20. Aronson E., Mills J. The Effect of Severity of Initiation on Liking for a Group. *Journal of Abnormal and Social Psychology*, 1959, vol. 59, no. 2, pp. 177–181. DOI: 10.1037/h0047195.
21. Kruger J., Wirtz D., Van Boven L., Altermatt T.W. The Effort Heuristic. *Journal of Experimental Social Psychology*, 2004, vol. 40, no. 1, pp. 91–98. DOI: 10.1016/S0022-1031(03)00065-9.
22. Sharot T. The Optimism Bias. *Current Biology*, 2011, vol. 21, no. 23, pp. R941–R945. DOI: 10.1016/j.cub.2011.10.030.

23. Lyu D., Jia F., Gai X. Optimism Bias, Judgment of Severity, and Behavioral Change During Two Stages of the Pandemics in China. *Scientific Reports*, 2025, vol. 15. URL: <https://doi.org/10.1038/s41598-024-84057-0>.
24. Chen C., Ishfaq M., Ashraf F., Sarfaraz A., Wang K. Mediating Role of Optimism Bias and Risk Perception Between Emotional Intelligence and Decision-Making: A Serial Mediation Model. *Frontiers in Psychology*, 2022, vol. 13. URL: <https://doi.org/10.3389/fpsyg.2022.914649>.
25. Helweg-Larsen M., Shepperd J.A. Do Moderators of the Optimistic Bias Affect Personal or Target Risk Estimates? A Review of the Literature. *Personality and Social Psychology Review*, 2001, vol. 5, no. 1, pp. 74–95. DOI: 10.1207/S15327957PSPR0501\_5.
26. Blanco F., Matute H., Vadiello M.A. Interaction Between the Illusion of Control and the Personal Involvement of the Participants. *Consciousness and Cognition*, 2012, vol. 21, no. 1, pp. 423–432. DOI: 10.1016/j.concog.2011.12.001.
27. Nickerson R.S. Confirmation Bias: A Ubiquitous Phenomenon in Many Guises. *Review of General Psychology*, 1998, vol. 2, no. 2, pp. 175–220. DOI: 10.1037/1089-2680.2.2.175.
28. Suzuki S., Yamamoto Y. Characterizing the Influence of Confirmation Bias on Web Search Behavior. *Frontiers in Psychology*, 2021, vol. 12. DOI: 10.3389/fpsyg.2021.771948.
29. Bornstein R.F., D'Agostino P.R. The Mere Exposure Effect: An Uncertainty Reduction Explanation Revisited. *Personality and Social Psychology Bulletin*, 1992, vol. 18, no. 1, pp. 130–139. DOI: 10.1177/0146167292181015.
30. Zavarykin I.N. *Crime Prevention: The Victimological Aspect*. Barnaul Law Institute of the Ministry of Internal Affairs of Russia Publ., 2021. 88 p.
31. Repetskaya A.L., Petryakova L.A. Criminological Analysis of the Current State of Fraud in the Banking Sector of Russia. *Vestnik Omskogo universiteta. Seriya: Pravo = Herald of Omsk University. Series: Law*, 2022, vol. 19, no. 1, pp. 62–72. (In Russian). EDN: PSPQXA. DOI: 10.24147/1990-5173.2022.19(1).62-72.
32. Zajonc R.B. Mere Exposure: A Gateway to the Subliminal. *Current Directions in Psychological Science*, 2001, vol. 10, no. 6, pp. 224–228. DOI: 10.1111/1467-8721.00154.

#### ИНФОРМАЦИЯ ОБ АВТОРАХ

Раднаева Эльвира Львовна — директор Института права и экономики Бурятского государственного университета имени Доржи Банзарова, кандидат юридических наук, доцент, г. Улан-Удэ, Российская Федерация; e-mail: [elvira.radnaeva@mail.ru](mailto:elvira.radnaeva@mail.ru),  <https://orcid.org/0000-0001-7089-4378>.

Семенова Наталья Александровна — преподаватель кафедры уголовного права, процесса и криминалистики Института права и экономики Бурятского государственного университета имени Доржи Банзарова, г. Улан-Удэ, Российская Федерация; e-mail: [624559@list.ru](mailto:624559@list.ru),  <https://orcid.org/0009-0004-3138-960X>.


#### ВКЛАД АВТОРОВ


Все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

#### ДЛЯ ЦИТИРОВАНИЯ

Раднаева Э.Л. Влияние когнитивных искажений на поведение жертв онлайн-мошенничеств и их учет при разработке мер виктимологической профилактики / Э.Л. Раднаева, Н.А. Семенова. — DOI 10.17150/2500-4255.2025.19(2).148-159. — EDN FENCHK // Всероссийский криминологический журнал. — 2025. — Т. 19, № 2. — С. 148–159.

#### INFORMATION ABOUT THE AUTHORS

Radnaeva, Elvira L. — Director, Institute of Law and Economics, Buryat State University named after D. Banzarov, Ph.D. in Law, Ass. Professor, Ulan-Ude, the Russian Federation; e-mail: [elvira.radnaeva@mail.ru](mailto:elvira.radnaeva@mail.ru),  <https://orcid.org/0000-0001-7089-4378>.

Semenova, Natalia A. — Lecturer, Department of Criminal Law, Procedure and Criminology, Institute of Law and Economics, Buryat State University named after D. Banzarov, Ulan-Ude, the Russian Federation; e-mail: [624559@list.ru](mailto:624559@list.ru),  <https://orcid.org/0009-0004-3138-960X>.

#### CONTRIBUTION OF THE AUTHORS

The authors contributed equally to this article. The authors declare no conflicts of interests.

#### FOR CITATION

Radnaeva E.L., Semenova N.A. Cognitive Biases Influencing the Behavior of Online Fraud Victims and Considering Them in the Development of Victimological Prevention Measures. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2025, vol. 19, no. 2, pp. 148–159. (In Russian). EDN: FENCHK. DOI: 10.17150/2500-4255.2025.19(2).148-159.