



ВИКТИМОЛОГИЧЕСКИЕ АСПЕКТЫ ПРЕСТУПНОСТИ (ВИКТИМОЛОГИЯ ПРЕСТУПНОСТИ)



Научная статья

УДК 343.988

DOI: 10.47475/2411-0590-2025-12-4-601-610

Виктимологический феномен мошенничества с использованием цифровых технологий социального инжиниринга

Юлия Михайловна Графова

*Казанский инновационный университет имени В. Г. Тимирязова, г. Казань, Россия
Grajia5@gmail.com*

Аннотация. *Введение.* В 2025 году киберпреступники осуществили хищение финансовых средств у граждан Российской Федерации в размере 55 миллиардов рублей, при этом около половины этой суммы было изъято с применением методов социальной инженерии. Злоумышленники активизируют свои действия в периоды экономических кризисов и чрезвычайных ситуаций, когда население испытывает повышенную тревожность и подвержено манипуляциям. Несмотря на наличие высокотехнологичных систем защиты информации, киберпреступники предпочитают использовать методы социальной инженерии для получения доступа к банковским данным. Эти методы основаны на психологических манипуляциях, направленных на вынуждение человека добровольно раскрыть конфиденциальную информацию, такую как логины, пароли, номера банковских карт и счетов. Полученная информация затем используется для осуществления финансовых операций без ведома владельца счета, что приводит к значительным материальным потерям.

Материалы и методы. В процессе исследования были использованы следующие методы: теоретический анализ научной литературы; эмпирические методы: диалектический; системно-структурный, направленный на выявление системных характеристик изучаемого феномена и взаимосвязей между его элементами.

Результаты исследования и их обсуждения. Наиболее распространенными методами социальной инженерии являются телефонное мошенничество и фишинг, каждый из которых имеет свои уникальные особенности и механизмы реализации. Телефонное мошенничество представляет собой форму киберпреступности, при которой злоумышленники устанавливают контакт с жертвой по телефону, используя заранее подготовленные сценарии, включающие психологические ловушки. Основной целью данного вида мошенничества является получение конфиденциальной информации, необходимой для несанкционированного доступа к банковским счетам и совершения финансовых операций.

Киберпреступники используют различные психологические приемы, такие как создание срочности, использование авторитетных имен и логотипов, а также технические методы, направленные на маскировку вредоносного контента. В результате жертва, не подозревая о подвохе, добровольно предоставляет свои конфиденциальные данные, которые затем используются для несанкционированных финансовых операций.

© Ю. М. Графова

Заключение. разработка и изучение проблем виктимизации граждан, ставших жертвами социально-инжиниринговых атак, может выступать основой для создания комплексных программ профилактики и предупреждения в сфере использования современных цифровых технологий.

Ключевые слова: виктимность, виктимологическая профилактика, кибермошенничество, социальный инженер, социальный инжиниринг, кибератака

Для цитирования: Графова Ю. М. Виктимологический феномен мошенничества с использованием цифровых технологий социального инжиниринга // Виктимология. 2025. Т. 12, № 4. С. 601–610. DOI: 10.47475/2411-0590-2025-12-4-601-610

Research article

Victimological Phenomenon of Fraud Using Digital Technologies of Social Engineering

Yulia M. Grafova

*Kazan Innovation University named after V. G. Timiryasova,
Kazan, Russia
Grajia5@gmail.com*

Abstract. Introduction. In 2025, cybercriminals stole 55 billion rubles from Russian citizens, with approximately half of this amount obtained using social engineering. Criminals intensify their activities during periods of economic crises and emergencies, when the population experiences heightened anxiety and is susceptible to manipulation. Despite the availability of high-tech information security systems, cybercriminals prefer to use social engineering to gain access to banking data. These methods rely on psychological manipulation aimed at coercing individuals into voluntarily revealing confidential information, such as logins, passwords, bank card numbers, and account numbers. The obtained information is then used to conduct financial transactions without the account holder's knowledge, resulting in significant financial losses. *Materials and Methods.* The following methods were used in the study: theoretical analysis of scientific literature; empirical dialectical methods; and a systemic-structural approach aimed at identifying the systemic characteristics of the phenomenon under study and the relationships between its elements. **Research Results and Discussion:**

The most common social engineering methods are telephone fraud and phishing, each with its own unique characteristics and implementation mechanisms. Telephone fraud is a form of cybercrime in which attackers contact victims by telephone using pre-arranged scenarios that incorporate psychological traps. The primary goal of this type of fraud is to obtain confidential information necessary for unauthorized access to bank accounts and financial transactions.

Cybercriminals employ various psychological techniques, such as creating urgency, using reputable names and logos, and technical methods aimed at disguising malicious content. As a result, the victim, unaware of the trap, voluntarily provides their confidential data, which is then used for unauthorized financial transactions.

Conclusion. The development and study of victimization issues in social engineering attacks can serve as the basis for the creation of comprehensive prevention and warning programs in the field of modern digital technologies.

Keywords: victimization, victimological prevention, cyberbullying, social engineering, social engineering, cyberattack

For citation: Grafova YuM. Victimological Phenomenon of Fraud Using Digital Technologies of Social Engineering. *Victimology*. 2025;12(4):601-610. DOI: 10.47475/2411-0590-2025-12-4-601-610 (In Russ.)

Введение

Социальная инженерия представляет собой методологический подход, основанный на применении психологических техник для манипуляции человеческим поведением. Основная цель данной манипуляции заключается в побуждении индивида к выполнению определенных действий или раскрытию конфиденциальной информации. Этот метод широко используется в сфере информационной безопасности, а также среди хакеров, однако его элементы находят применение и в повседневной жизни [8].

В бизнес-среде, например, отделы продаж и маркетинга активно интегрируют техники социальной инженерии в свою практику. Торговые представители, осуществляющие обзвон потенциальных клиентов, применяют различные стратегии для воздействия на их решения. В детской среде также наблюдается использование приемов социальной инженерии [10], направленных на достижение желаемого результата от родителей. Родители, в свою очередь, прибегают к аналогичным методам, преувеличивая негативные последствия для достижения желаемого изменения в поведении ребенка (например, используя страх перед последствиями чрезмерного потребления сладкого для формирования более здоровых пищевых привычек).

Актуальность темы исследования подтверждают следующие статистические данные: за 2024 год в Российской Федерации число лиц, осужденных по ст. 159 УК РФ составило 27 916 человек; за 2023 год — 27 483 человек; за 2022 год — 23 738 человек; за 2021 год — 22 718 человек¹.

По данным МВД России, в 2024 году количество уголовных дел, направленных с обвинительным заключением в суды

по ст. 159 УК РФ о мошенничестве, увеличилось на 2,1 % и составило 32,9 тыс. преступлений. При этом общая раскрываемость мошенничества в сфере компьютерной информации — 23,2 %, непосредственно мошенничеств — 10,1 %. Также известно, что в 2024 году количество преступлений с применением мошеннических действий стало на 15 % больше, чем в 2023 году².

В контексте социальной инженерии термин «претекст» («pretexting») представляет собой метод [5], при котором индивид симулирует свою идентичность, выдавая себя за другое лицо. Данный подход может включать в себя использование альтернативных атрибутов, таких как профессиональная униформа, создание вымышленной биографической предыстории или формирование фиктивных обстоятельств для инициирования контакта.

Какой бы совершенной ни была система безопасности, в ней есть как минимум одна серьезная уязвимость — человек. Именно им, вернее, человеческими слабостями (доверие, страх, спешка, неуверенность или жажда помощи) манипулируют социальные инженеры, большая часть из которых — мошенники). Цель такого поведения — получить доступ к конфиденциальной информации, ресурсам или системам, минуя технические средства защиты. Злоумышленники, как правило, выбирают стратегию воздействия на когнитивные процессы и эмоциональные состояния индивидов, а не на технические аспекты их компьютерных систем [4]. Они применяют различные методы манипуляции сознанием, эксплуатируя психологические слабости и уязвимости человека с целью побудить его к добровольному раскрытию конфиденциальной информации или выполнению требуемых действий. Данный подход, известный как социальная инженерия, позволяет киберпреступникам обходить техниче-

¹ Судебная статистика Российской Федерации. — Режим доступа: <https://stat.апи-пресс.рф/> (Дата обращения 10.04.2025 г.).

² Там же.

ские барьеры безопасности и эффективно использовать человеческий фактор в своих целях [6].

Вот 15 наиболее распространенных методов, которые они применяют:

1. Создание чувства срочности.
2. Игра на эмоциях (страх, вина, радость).
3. Использование авторитетов.
4. Ложное доверие.
5. Обманчивые обещания.
6. Психологическое давление.
7. Поток информации (информационный перегруз).
8. Социальное доказательство (подтверждение от «друзей»).
9. Деформация реальности (искажение фактов).
10. Недостаток сна и отдыха.
11. Скрытая манипуляция через вопросы.
12. Использование фальшивых идентичностей.
13. Эмоциональная привязка.
14. Создание иллюзии выбора.
15. Демонстрация «эксклюзивности» предложения.

В кибератаках — чтобы получить логины, пароли, доступ к системам.

В офлайн-среде — например, проникновение на охраняемый объект под видом сотрудника.

В корпоративной среде — для получения доступа к внутренним данным компаний.

В мошенничестве — звонки от «службы безопасности», SMS о «выигрыше», просьбы о помощи, доставка цветов и так далее.

Методология и методы

Методологическую основу исследования составляет комплекс общенаучных и специальных методов познания: диалектический, позволяющий рассмотреть цифровые технологии социального инжиниринга для совершения различных видов мошенничества как динамично развивающееся явление в единстве его противоречий; системно-структурный, направленный

на выявление системных характеристик изучаемого феномена и взаимосвязей между его элементами; формально-логический, обеспечивающий категориально-понятийную определенность исследования; компаративистский, позволяющий сопоставить различные проявления кибермошенничества в различных контекстах; прогностический, направленный на моделирование перспектив развития социального инжиниринга.

Результаты исследования и их обсуждение

Основная цель цифровой виктимологии заключается в минимизации уровня кибервиктимности посредством применения современных и этически обоснованных методов виктимологического воздействия, направленных на предотвращение и пресечение киберпреступности. Данный подход характеризуется высокой эффективностью при относительно низких материальных затратах и основывается на внутренней мотивации индивида к самозащите и обеспечению информационной безопасности [2].

Для корректного понимания направлений виктимологической деятельности в цифровом пространстве необходимо дать определение термину «киберпреступность». В контексте современных информационных технологий под киберпреступностью понимается любая противоправная деятельность, осуществляемая с использованием компьютера, компьютерной сети или иных сетевых устройств. Большинство киберпреступлений имеют корыстную мотивацию, направленную на получение финансовой выгоды, однако значительная часть таких правонарушений преследует цели нарушения функционирования компьютерных систем, что может быть обусловлено личными, политическими или иными мотивами [7].

Киберпреступность представляет собой сложное и многогранное явление, требующее комплексного подхода к её изучению и противодействию. В рамках цифровой виктимологии особое внимание уделяется

анализу факторов, способствующих виктимизации индивидов в цифровом пространстве, а также разработке стратегий и методов защиты, направленных на минимизацию рисков и повышение уровня информационной грамотности населения, в том числе профилактике жертв атак социальных инженеров. Таким образом, цифровая виктимология играет ключевую роль в формировании культуры информационной безопасности и снижении уровня кибервиктимности, что является важным аспектом обеспечения устойчивого развития информационного общества.

В современном мире, когда активно реализуются новые технологии, используются ресурсы повышенной опасности, по статистическим данным можно наблюдать возрастание мошеннических действий в Российской Федерации из года в год.

В процессе развития уголовного законодательства об ответственности за совершение мошеннических посягательств законодатель непрерывно старается раскрывать существенные признаки мошенничества. Однако, вводя новые термины, он не всегда даёт им удачное толкование, в связи с чем на практике возникают проблемы при реализации норм уголовного права.

В контексте философской антропологии и психологии С. Дерябо вводит термин «субъектность», который является фундаментальным концептом, определяющим сущность субъекта и его отличие от объектов и других субъектов [3]. Субъектность, по мнению С. Дерябо, представляет собой интегральное качество, характеризующее способность субъекта к активной и осознанной деятельности в рамках жизненного процесса. Это качество предполагает не только взаимодействие с внешней средой и другими индивидами, но и рефлексивное отношение к самому себе, что позволяет субъекту выступать в качестве активного участника и творца своего бытия [3].

В данном исследовании мы будем рассматривать субъектность как комплексную когнитивно-поведенческую структу-

ру, определяющую субъекта как активного деятеля, способного к самодетерминации, самосознанию и саморефлексии. Таким образом, субъектность выступает как ключевой феномен, определяющий качественную специфику субъектно-объектных отношений и способствующий пониманию природы человеческого существования в контексте его взаимодействия с окружающей средой и социальным контекстом.

Мошенничество представляет собой манипулятивное воздействие на жертву, вследствие которого она выполняет действия, предварительно спланированные злоумышленником. В данном контексте ответственность с жертвы фактически снимается, поскольку она оказывается объектом внешнего влияния, не обладающим достаточной степенью свободы выбора в данной ситуации. Однако, с иной перспективы, жертва проявляет свою субъектность через конкретные действия, осуществляемые в рамках преступного взаимодействия. Субъектность жертвы актуализируется в момент принятия решения о взаимодействии с мошенником, что предполагает осознанный выбор в пользу продолжения коммуникации, а не избегания её. Таким образом, феномен мошенничества можно рассматривать как сложное взаимодействие между манипулятивным воздействием и субъективными реакциями жертвы, где каждый из участников демонстрирует свою степень автономности и ответственности.

Личность, осознающая многогранность своего положения и принимающая на себя все потенциальные риски, приобретает статус субъекта. Данный аспект приобретает особую значимость в контексте индивидов, ранее сталкивавшихся с аналогичными ситуациями или подвергавшихся мошенническим действиям. Субъективность жертвы проявляется в феномене игнорирования собственных личностных характеристик, которые могли бы способствовать её виктимизации [9]. Личность жертвы социального инженера представляет собой комплексную структуру, включающую психологические

и моральные аспекты, социально-демографические и социально-ролевые параметры, а также взаимоотношения с причинителем вреда и её роль в механизме совершения преступления.

Для индивидов, оказавшихся жертвами мошеннических действий, следует учитывать комплекс психологических, когнитивных и социальных факторов, которые детерминируют их уязвимость к подобного рода преступлениям. Среди ключевых предикторов можно выделить склонность к рисковому поведению, уровень доверчивости, простоту характера, когнитивные способности, включая способность к критической оценке ситуации и своевременной остановке, а также коммуникативные навыки, способствующие сопротивлению мошенническим схемам.

Когнитивные и личностные характеристики, такие как мировоззрение, жизненные цели и ценностные ориентации, играют существенную роль в формировании поведенческих паттернов, связанных с взаимодействием с мошенническими элементами. Важно проанализировать, как индивид соотносит средства и цели, насколько он готов к использованию незаконных методов, стремится ли к быстрой и легкой наживе, а также учитывает ли интересы других людей в своих действиях [9].

Социальные и психологические установки, взгляды и убеждения человека, а также его отношение к окружающим и уровень доверия к различным институтам оказывают значительное влияние на его поведение в ситуациях, предшествующих мошенничеству, во время его совершения и после. Необходимо учитывать, будет ли человек вступать во взаимодействие с мошенником, способен ли он распознать нечестность и прекратить контакт, а также обратится ли за помощью, включая обращение в правоохранительные органы.

Таким образом, комплексный анализ вышеуказанных факторов позволяет более глубоко понять механизмы, лежащие в основе уязвимости индивидов к мошенническим действиям, и разработать эффек-

тивные стратегии профилактики и противодействия этим преступлениям.

Р. Титус выдвигает гипотезу о том, что потенциальная жертва может невольно способствовать реализации мошеннических схем, совершая определённые действия, которые создают благоприятные условия для преступника. Во-первых, жертва может инициировать контакт с преступником или предпринять шаги, способствующие такому взаимодействию, раскрывая информацию о своём местонахождении и демонстрируя готовность к сотрудничеству [11]. Во-вторых, потенциальная жертва может предоставить преступнику конфиденциальные данные, которые могут быть использованы для реализации мошеннических замыслов. В-третьих, жертва может способствовать трансформации деловых отношений в личные, создавая доверительную атмосферу и отказываясь от стандартных мер предосторожности. В-четвёртых, жертва может ненамеренно содействовать созданию сценария событий, который выглядит правдоподобно и служит основой для мошеннической схемы. Наконец, жертва может предоставить преступнику доступ к своим финансовым ресурсам, например, посредством выписки чека, передачи кредитной карты или раскрытия номера банковского счёта.

С точки зрения Э. Берна, любое взаимодействие, даже если оно приводит к негативным результатам, имеет ценность для индивида. Берна рассматривает общение как процесс обмена «поглаживаниями», то есть актами, которые подтверждают присутствие другого человека [1]. Таким образом, жертва мошенничества, независимо от исхода, получает внимание и опыт, которые могут быть использованы в будущем. Хотя жертва может воспринимать утрату как значительный ущерб, она также извлекает пользу из самого факта общения. Подсознательно жертва может стремиться к обману, поскольку это позволяет ей получить «поглаживания». Однако разочарование вызывает не сам факт обмана, а неспособность адекватно оценить риски и свои возмож-

ности. В случае незначительного ущерба жертва может не испытывать сильного беспокойства по поводу произошедшего.

Ещё одной причиной, по которой жертва может извлечь выгоду из общения с мошенником, является ожидание «поглаживаний» со стороны окружающих. Родственники, знакомые и даже представители правоохранительных органов могут проявить повышенное внимание к пострадавшему. В обществе существует стереотип, что жертва — это проигравший, которому необходима помощь, что может выражаться в форме сочувствия и заботы.

В условиях доминирования данного стереотипа в социуме, жертва демонстрирует уверенность в достижении своих ожиданий. Преступник, жертва и контекстуальные обстоятельства формируют целостную систему, функционирование которой детерминировано наличием всех этих компонентов. В контексте реализации мошеннических схем жертва не выступает в роли пассивного объекта, через который преступник осуществляет свои корыстные намерения. Напротив, она является активным субъектом, участвующим в динамике событий и влияющим на их развитие.

В случае, когда поведение потенциальной жертвы демонстрирует низкий уровень виктимности, обусловленный адекватным уровнем личной имущественной и информационной безопасности, преступные элементы прибегают к использованию сложных и изощренных методов для преодоления стандартных и высокозащищенных систем безопасности. Эти методы включают комплексное воздействие на средства обработки, хранения и передачи данных, что требует проведения тщательной подготовки, включая анализ потенциальных уязвимостей, выбор объектов нападения и разработку соответствующих стратегий воздействия.

В условиях, когда поведение жертвы может быть классифицировано как умеренно виктимное вследствие недостаточной имплементации мер имущественной и информационной безопасности, а также игнори-

рования ключевых аспектов обеспечения кибербезопасности, злоумышленники прибегают к сложным и изощренным техникам для обхода стандартных защитных механизмов. Эти преступники направляют свои усилия на эксплуатацию уязвимостей в системах обработки, хранения и передачи данных, что позволяет им манипулировать функциональностью указанных систем [7].

В рамках своих операций злоумышленники применяют типовые стратегии, ориентированные на идентификацию и последующую эксплуатацию потенциальных уязвимостей в информационной инфраструктуре потенциальных жертв. Данный подход позволяет им систематически осуществлять киберпреступления, демонстрируя высокий уровень профессионализма и технической компетентности.

Заключение

Мошеннические действия представляют собой серьезную угрозу как для отдельных граждан, так и для экономической системы Российской Федерации. В современном правовом контексте наблюдаются значительные сложности в определении состава мошенничества, особенно в аспекте приобретения права на чужое имущество. Существующие юридические доктрины не предлагают единого подхода к интерпретации понятия корыстной цели, что вызывает неоднозначность в правоприменительной практике. Кроме того, дискуссионным остается вопрос о целесообразности и эффективности смягчения уголовной ответственности за данное правонарушение. Конституция РФ провозгласила права и свободы человека высшей ценностью, обеспечиваемой правосудием, и возложила на государство обязанность соблюдать и защищать права человека. Это говорит о том, что Российская Федерация не только признает основные права, но и декларирует защиту прав и свобод своих граждан в качестве одной из приоритетных государственных функций.

Мошенничество представляет собой комплексную и многоаспектную катего-

рию преступлений, характеризующуюся высокой степенью адаптивности и многообразием форм проявления. Его уникальные свойства и специфические особенности позволяют выделить мошенничество среди прочих видов правонарушений, что обусловлено его способностью к трансформации и эволюции в ответ на изменения в социальной, экономической и технологической среде.

Широкие возможности использования ресурсов сети Интернет и средств мобильной связи коренным образом изменили традиционные способы взаимодействия преступника и жертвы, ведущим из которых стало дистанционное взаимодействие. Именно освоению механизмов такого воздействия на потенциальную жертву, использованию технологий социальной инженерии преступники уделяют основное внимание. В рассматриваемой ситуации жертва преступления занимает центральное положение в механизме преступления, именно от ее поведения (зачастую прогнозируемого, моделируемого и управляемого преступником) во многом зависит успех противоправной деятельности.

Однако сложившаяся в настоящее время правоохранительная практика ориентирована в основном на посткриминальную реакцию уголовно-процессуальными средствами на возрастающий массив дистанционных хищений и не способна качественно образом переломить негативные тенденции. Вместе с тем, с учетом низкой эффективности карательной политики и в силу высокой роли жертвы в механиз-

ме совершения большинства указанных преступлений, наибольший антикриминальный потенциал заложен в построении системы виктимологического предупреждения дистанционных хищений.

Несмотря на усиливающиеся риски и угрозы безопасности в данной сфере, адекватная и своевременная оценка рассматриваемым тенденциям и закономерностям в криминологической науке по-прежнему не дана; в предметном поле криминологии не представлена исчерпывающая актуальная информация о характеристике дистанционных хищений и личности их жертв, механизме и детерминантах их совершения. Отмечается острый дефицит научной информации в области теории виктимологического предупреждения указанных преступлений, что лишает практику научно обоснованных рекомендаций по выстраиванию и совершенствованию системы предупредительной деятельности в данной сфере.

В условиях, когда поведение потенциальной жертвы характеризуется высокой степенью виктимности, обусловленной игнорированием или недостаточным пониманием принципов обеспечения имущественной и информационной безопасности, злоумышленники могут эффективно эксплуатировать уязвимости в системе защиты, созданные самим субъектом. Данный феномен обусловлен отсутствием базовых знаний в области кибербезопасности, а также наличием свободного доступа к объектам, подверженным кибератакам.

Список источников

1. Берн Э. Игры, в которые играют люди. Люди, которые играют в игры. Москва: Современный литератор, 2006. 340 с.
2. Вострецова Е. В. Основы информационной безопасности. Екатеринбург, 2019. 204 с.
3. Дерябо С. Личность: от субъективности к субъектности // Развитие личности. 2002. № 3. С. 261–265.
4. Игнатова Е. С. Манипуляция эмоциональной безопасностью кибермошенниками с применением технологий социальной инженерии: case-study // Вестник Пермского университета. Философия. Психология. Социология. 2024. Вып. 3. С. 374–390. DOI: <https://doi.org/10.17072/2078-7898/2024-3-374-390>.

5. Маркелов В. К., Привалов А. Н. Метод претекстинга как угроза информационной безопасности в социальных сетях // Вестник Адыгейского государственного университета. Сер.: Естественно-математические и технические науки. 2024. Вып. 2 (341). С. 51–61. DOI: <https://doi.org/10.53598/2410-3225-2024-2-341-51-61>
6. Мельников А. И. Социальная инженерия в цифровой эпохе: анализ методов манипуляции человеческим фактором в целях кибератак // Социально-гуманитарные знания. 2024. № 1. С. 50–54.
7. Попов А. Ю. Эмпирическое исследование процессов субъект-субъектного взаимодействия людей: принципы и первые результаты // Психология. Психофизиология. 2011. № 5(222). С. 42–47.
8. Ткачева М. В. Средства и методы защиты информации в рамках обеспечения экономической безопасности организации: основная характеристика // Современная экономика: проблемы и решения. 2024. № 5(173). С. 165–177. DOI: <https://doi.org/10.17308/meps/2078-9017/2024/5/165-177>.
9. Фоминых Е. С. Психологические механизмы виктимности // Научно-методический электронный журнал «Концепт». 2014. № 5. С. 116–120.
10. Худайберганов Т. Р., Курбонбоев К. А., Холлиев С. Х. Социальная инженерия и школы: разработка способов защиты учащихся от манипуляций // Universum: технические науки: электрон. научн. журн. 2025. № 4(133). URL: <https://7universum.com/ru/tech/archive/item/19824>
11. Titus R., Gover A. Personal Fraud: The Victims and the Scams. In G. Farrell and K. Pease (eds.), *Repeat Victimization, Crime Prevention Studies*, 2001. Vol. 12 Monsey, N.Y.: Criminal Justice Press. URL: <http://www.springerlink.com/content/q3582003t7p476j6/> (дата обращения: 22.11.2025).

References

1. Bern E. *Games that people play. People who play games*. Moscow; 2006. 340 p. (In Russ.).
2. Vostretsova EV. *Fundamentals of information security*. Yekaterinburg; 2019. 204 p. (In Russ.).
3. Deryabo S. Personality: from subjectivity to subjectivity. *Personality development*. 2002;(3):261–265. (In Russ.).
4. Ignatova ES. Manipulation of emotional security by cybercriminals using social engineering technologies: a case study. *Bulletin of Perm University. Philosophy. Psychology. Sociology*. 2024;(3):374–390. (In Russ.). DOI: <https://doi.org/10.17072/2078-7898/2024-3-374-390>
5. Markelov VK, Privalov AN. The method of pretexting as a threat to information security in social networks. *Bulletin of the Adygea State University. Ser.: Natural, mathematical and technical sciences*. 2024;(2):51–61. (In Russ.). DOI: <https://doi.org/10.53598/2410-3225-2024-2-341-51-61>
6. Melnikov AI. Social engineering in the digital age: analysis of methods of manipulation of the human factor for the purposes of cyber attacks. *Socio-humanitarian knowledge*. 2024;(1):50–54. (In Russ.).
7. Popov AYu. Empirical research of the processes of subject-subject interaction of people: principles and first results. *Psychology. Psychophysiology*. 2011;(5):42–47. (In Russ.).
8. Tkacheva MV. Information security tools and methods for ensuring an organization's economic security: key characteristics. *Modern economics: problems and solutions*. 2024;(5):165–177. (In Russ.). DOI: <https://doi.org/10.17308/meps/2078-9017/2024/5/165-177>.
9. Fominih ES. Psychological mechanisms of victimization. *Scientific and methodological electronic journal "Concept"*. 2014;(5):116–120. (In Russ.).
10. Khudaiberganov TR, Kurbonboev KA, Kholliiev SK. Social engineering and schools: developing ways to protect students from manipulation. *Universum*. 2025;(4). URL: <https://7universum.com/ru/tech/archive/item/19824> (In Russ.).
11. Titus R, Gover A. Personal Fraud: The Victims and the Scams. In G. Farrell and K. Pease (eds.), *Repeat Victimization, Crime Prevention Studies*. 2001. Vol. 12 Monsey, N.Y.: Criminal Justice Press. URL: <http://www.springerlink.com/content/q3582003t7p476j6/>

ИНФОРМАЦИЯ ОБ АВТОРЕ

Графова Юлия Михайловна

Адвокат, психолог, руководитель НКО «Человек и Закон»;
соискатель

Казанский инновационный университет имени В. Г. Тимирязова, 420111, Россия, г. Казань, ул. Московская д. 42

Grajia5@gmail.com

INFORMATION ABOUT THE AUTHOR

Yulia M. Grafova

Lawyer, Psychologist, Head of NGO "Man and the Law";
Kazan Innovative University named after V. G. Timiryasov,
42 Moskovskaya str., Kazan 420111, Russia.

Grajia5@gmail.com

КОНФЛИКТ ИНТЕРЕСОВ

Конфликт интересов отсутствует.

CONFLICT OF INTEREST

There is no conflict of interest.

Дата поступления статьи / Received: 08.12.2025.

Дата рецензирования статьи / Revised: 19.12.2025.

Дата принятия статьи к публикации / Accepted: 22.12.2025.