Научная статья
УДК 343.988:004

Людмила Александровна Голубева
Санкт-Петербургский университет МВД России, Санкт-Петербург, Россия, ludmigol.official@gmail.com

ХАРАКТЕРНЫЕ ОСОБЕННОСТИ ЛИЧНОСТИ ЖЕРТВЫ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. Статья посвящена анализу характерных особенностей личности жертвы преступлений в сфере информационно-коммуникационных технологий (далее – ИКТ). Автор обосновывает введение и использование термина «жертва» вместо «потерпевший», подчеркивая специфику виктимизации в цифровой среде. В работе детально рассмотрены виктимогенные факторы поведения, выделены типичные модели поведения жертв ИКТ-преступлений. Проведена оценка виктимного потенциала различных социально-демографических групп. Ключевое внимание уделено анализу факторов виктимности и методам социальной инженерии как основному инструменту злоумышленников; представлена авторская модель этапов применения социальной инженерии. Исследование подчеркивает актуальность и необходимость дальнейшего углубленного изучения психологических и поведенческих аспектов виктимности в контексте постоянно эволюционирующих ИКТ-угроз для разработки эффективных профилактических мер.

Ключевые слова: жертвы ИКТ-преступлений, виктимность личности, виктимогенные факторы, модели поведения жертв, социальная инженерия, виктимный потенциал, информационно-коммуникационные технологии

Для цитирования: Голубева Л. А. Характерные особенности личности жертвы преступлений в сфере информационно-коммуникационных технологий // Общество, право, государственность: ретроспектива и перспектива. 2026. № 1 (25). С. 39–48.

Original article

Lyudmila A. Golubeva
Saint Petersburg University of the Ministry of Internal Affairs of Russia, Saint Petersburg, Russia, ludmigol.official@gmail.com

CHARACTERISTIC FEATURES OF THE PERSONALITY OF THE VICTIM OF CRIMES IN THE FIELD OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Abstract. The article is devoted to the analysis of the characteristic features of the personality of the victim of crimes in the field of information and communication technologies (ICT). The author justifies the introduction and use of the term “victim” instead of “complainant”, emphasizing the specifics of victimization in the digital environment. The paper considers victimogenic factors of behavior in detail, identifies typical patterns of behavior of victims of ICT crimes. The victim potential of various socio-demographic groups has been assessed. Key attention is paid to the analysis of victimization factors and social engineering methods as the main tool of intruders; the author’s model of the stages of social engineering application is presented. The study highlights the relevance and necessity of further in-depth study of the psychological and behavioral aspects of victimization in the context of constantly evolving ICT threats in order to develop effective preventive measures.

Keywords: victims of ICT crimes, personal victimization, victimogenic factors, victim behavior patterns, social engineering, victim potential, information and communication technologies

For citation: Golubeva L. A. Characteristic features of the personality of the victim of crimes in the field of information and communication technologies // Society, law, statehood: retrospective and perspective. 2026. No. 1 (25). P. 39–48. (In Russ.)

Введение

В современном мире, где информационно-коммуникационные технологии (далее – ИКТ) становятся неотъемлемой частью повседневной жизни, преступления, совершенные с их использованием, приобретают все более актуальный характер. Однако любое преступление, независимо от его природы и методов совершения, не обходится без жертвы. Традиционно в криминологии акцент делается на криминогенных факторах – условиях и обстоятельствах, способствующих совершению преступлений. Тем не менее для более глубокого понимания механизма преступности необходимо также рассматривать виктимогенные факторы, которые включают в себя особенности личности жертвы.

Исследование личностных характеристик жертв преступлений, связанных с информационно-коммуникационными технологиями, позволяет выявить определенные паттерны и уязвимости, которые могут быть использованы преступниками. Психологические аспекты, такие как уровень доверчивости, социальная изоляция или недостаток цифровой грамотности, могут существенно влиять на вероятность того, что индивид станет жертвой. Понимание этих особенностей не только помогает в разработке более эффективных стратегий противодействия преступлениям, но и способствует формированию профилактических мер, направленных на защиту потенциальных жертв.

Методы

Автором при написании данной статьи использовались: метод системного анализа, статистический анализ, контент-анализ, описательный метод, а также другие общенаучные методы познания.

Результаты

Традиционный криминологический подход фокусируется преимущественно на анализе личности преступника, его мотивах, способах совершения преступления и мерах по его задержанию и наказанию. Однако для эффективной борьбы с преступностью, особенно в быстро развивающейся сфере информационно-коммуникационных технологий, следует уделять пристальное внимание и виктимологическому аспекту. Иными словами, необходимо изучать не только преступника, но и жертву преступления, ее характеристики, поведение и обстоятельства, сделавшие ее уязвимой.

Прежде чем говорить о характерных особенностях личности жертвы преступлений в сфере информационно-коммуникационных технологий, принципиально важно определить, кого мы относим к данной категории.

В современной науке вопрос об определении понятия «жертва преступления» является предметом активного обсуждения среди исследователей в области криминологии, виктимологии и уголовного права. Такие ученые, как Л. В. Франк, Х. Хентиг, Н. В. Щедрин, Д. В. Ривман и др., внесли значительный вклад в разработку данного термина, раскрывая его содержание с различных позиций.

Еще этнограф и лингвист В. И. Даль дал определение жертвы как «пожираемое, уничтожаемое, гибнущее»[1], а Д. Н. Ушаков как «человек, подвергнувшийся чьему-либо насилию, злому умыслу, пострадавший от кого-, чего-нибудь»[2]. Наиболее распространенным в научной литературе является определение жертвы преступления как физического или юридического лица, которому преступлением причинен физический, материальный или моральный вред. Это

[1] Толковый словарь живого великорусского языка: в 4 т. / сочинение Владимира Даля. М. : Издание Общества любителей российской словесности, учрежденного при Императорском Московском университете, 1863–1866. Т. 1. С. 1332.

[2] Ушаков Д. Н. Толковый словарь русского языка. Л., 1935. Т. 1. С. 860.

определение представляется рациональным, поскольку охватывает широкий спектр последствий преступных деяний и учитывает как индивидуальных, так и коллективных потерпевших. Оно также соответствует современным подходам виктимологии, ориентированным на защиту прав пострадавших и анализ их роли в механизме преступления.

Выбор термина «жертва преступления» вместо «потерпевший» в данном исследовании обусловлен несколькими причинами.

Во-первых, понятие «жертва» шире по своему содержанию и охватывает не только процессуальный статус лица в рамках уголовного судопроизводства (как термин «потерпевший»), но и социально-психологические аспекты, связанные с последствиями преступления. В то время как «потерпевший» – это юридическая категория, закрепленная в уголовно-процессуальном законодательстве и предполагающая формальное признание лица таковым в рамках возбужденного дела, «жертва» может рассматриваться еще до возбуждения уголовного дела или даже в случаях, когда преступление осталось незарегистрированным.

Во-вторых, термин «жертва» активно используется в виктимологии [1] – науке, изучающей поведение, роль и последствия для лиц, пострадавших от преступлений. Это позволяет анализировать не только правовые, но и криминологические, психологические и социальные аспекты виктимизации.

Наконец, в международных документах (например, в Декларации основных принципов правосудия для жертв преступлений и злоупотребления властью Организации Объединенных Наций 1985 г.[1]) используется именно понятие «жертва», что подчеркивает его универсальность и применимость в сравнительно-правовых исследованиях.

Таким образом, использование термина «жертва преступления» в настоящем исследовании позволяет выйти за рамки строго процессуального подхода и рассмотреть проблему комплексно, с учетом не только юридических, но и социально-криминологических аспектов.

Однако применительно к преступлениям, совершаемым с использованием информационно-коммуникационных технологий, традиционное понимание жертвы требует уточнения и адаптации. Это связано со спецификой данных преступлений, которая характеризуется трансграничностью, анонимностью злоумышленников, особыми способами причинения вреда и высокой латентностью. В связи с этим возникает необходимость разработки более узкого, но при этом содержательного определения, которое отражало бы ключевые особенности жертвы именно такого рода преступлений.

Для формулировки авторского определения целесообразно учитывать такие аспекты, как специфика вреда, способы виктимизации и особый статус жертвы.

Так, в отличие от традиционных преступлений, вред жертвам ИКТ-преступлений чаще всего носит имущественный, репутационный или психологический характер, а также может выражаться в нарушении конфиденциальности данных. Помимо этого, потерпевшие в цифровой среде часто не имеют непосредственного контакта с преступником, а их взаимодействие опосредовано техническими средствами, что влияет на восприятие и осознание факта виктимизации.

На основе анализа существующих подходов и с учетом указанных особенностей жертву преступления, совершенного с использованием информационно-коммуникационных технологий, можно определить как физическое или юридическое лицо, которому в результате умышленных противоправных действий, осуществляемых с применением цифровых технологий, причинен имущественный, моральный вред, нарушены права на конфиденциальность данных или нанесен ущерб репутации.

[1] Декларация основных принципов правосудия для жертв преступлений и злоупотребления властью : принята резолюцией 40/34 Генер. Ассамблеи ООН от 29 нояб. 1985 г. // ООН. URL: https://www.un.org/ru/documents/decl_conv/declarations/power.shtml (дата обращения: 10.05.2025).

Особенности взаимодействия преступника и жертвы в сфере информационно-коммуникационных технологий формируют уникальную систему криминогенных и виктимогенных факторов.

Криминогенные факторы цифровой среды включают ряд ключевых особенностей, способствующих совершению ИКТ-преступлений. Так, анонимность и трансграничность позволяют преступникам скрывать личность и географическое положение, что значительно снижает психологический барьер и риск разоблачения. Автоматизация атак с применением вредоносного программного обеспечения (далее – ПО) (включая бот-сети) дает возможность одновременно нацеливаться на тысячи потенциальных жертв с минимальными трудозатратами. А постоянно усложняющиеся методы атак, такие как фишинг, социальная инженерия и эксплуатация уязвимостей, требуют от жертв специальных знаний для распознавания угроз, что создает техническую сложность защиты. Кроме того, высокая доходность рассматриваемых преступлений при относительно низких рисках служит значительной экономической мотивацией для их распространения.

Со стороны жертвы можно выделить несколько виктимогенных факторов поведения, повышающих вероятность виктимизации. Цифровая неграмотность, выражающаяся в недостатке знаний о киберугрозах и способах защиты, делает пользователей уязвимыми перед элементарными схемами обмана. Психологические особенности, такие как доверчивость, излишняя уверенность в своей безопасности и импульсивность (например, клики по подозрительным ссылкам из любопытства), также способствуют виктимизации. Поведенческие паттерны в виде использования слабых паролей, пренебрежения обновлением ПО и привычки делиться личной информацией в соцсетях создают дополнительные риски. Особую группу риска составляют сотрудники организаций, работающие с финансами или персональными данными, которые часто становятся целями целенаправленных атак, таких как таргетированный фишинг или CEO-мошенничество.

В отличие от традиционных преступлений с непосредственным контактом между преступником и жертвой, в цифровой среде такое взаимодействие опосредовано технологиями и развивается по различным сценариям. Таргетированные атаки предполагают тщательное изучение жертвы через соцсети для персонализации атаки и повышения ее эффективности. Некоторые схемы, такие как romance scams (любовная афера), основаны на длительном контакте и постепенном «разогревании» жертвы через продолжительное общение.

Анализ современных угроз в сфере информационно-коммуникационных технологий позволяет выделить несколько типичных моделей поведения жертв:

1. Жертвы с *пассивной виктимностью* не осознают рисков или не предпринимают действий для их минимизации [2, с. 30]. К данной категории относятся неосведомленные пользователи, то есть лица, не обладающие достаточной цифровой грамотностью, чтобы распознать фишинг, мошеннические сайты или вредоносные программы (например, жертвы фишинговых атак, которые не проверяют URL-адреса или вводят конфиденциальные данные на поддельных страницах).

2. В модель *активной виктимности* входят жертвы, чьи действия прямо способствуют совершению преступления, например доверчивые жертвы, перечисляющие деньги мошенникам под предлогом помощи родственникам или выигрыша в лотерее. Такие жертвы часто игнорируют очевидные признаки обмана из-за эмоциональной вовлеченности, так как традиционно эффективная манипуляция строится на обнаружении и последующем использовании человеческой слабости, которая кроется в эмоциональной уязвимости личности [3, с. 378]. Также можно включить сотрудников организаций, которые пересылают конфиденциальные данные через незащищенные каналы или открывают вложения в подозрительных письмах, что приводит к утечке информации.

3. Учитывая предыдущие модели, можно выделить *смешанную*. К данной модели можно отнести такой факт, как игнорирование различных предупреждений. Например, жертвы могут видеть признаки мошенничества (как грамматические ошибки в письмах), но все равно совершают действия, ведущие к ущербу.

4. Модель провоцирующего поведения играет значительную роль в процессе виктимизации, при котором жертва, осознанно или неосознанно, создает условия, облегчающие осуществление преступных действий. В частности, раскрытие избыточной персональной информации в социальных сетях, включая данные документов, финансовую информацию и подробности личной жизни, способствует формированию цифрового профиля, который может быть использован для проведения целенаправленных атак. В массе потенциальных жертв злоумышленник будет искать того, кто привлекает внимание и будет откликаться на заданный сценарий [4, с. 213]. Следует отметить, что хотя указанные сведения могут быть получены злоумышленниками из альтернативных источников, таких как утечки данных и ресурсы сети Даркнет, добровольное предоставление информации пользователем существенно снижает порог реализации атак социальной инженерии, так как предоставляет злоумышленникам верифицированные и актуальные данные.

5. Последнюю модель можно отнести к *профессиональной виктимности*, поскольку люди могут в связи со своей профессиональной деятельностью обладать необходимой информацией для злоумышленников.

Так, мы можем видеть, что виктимность в цифровой среде зависит не только от личностных качеств жертвы, но и от контекста взаимодействия с технологиями.

Исследования в области виктимологии и юридической психологии демонстрируют, что психологические особенности жертв играют ключевую роль в их уязвимости к различным видам ИКТ-преступлений, поэтому можно проследить взаимосвязь между психологическими профилями жертв и спецификой преступлений, совершенных с использованием информационно-коммуникационных технологий. К примеру, лица, характеризующиеся низким самоконтролем, импульсивностью, склонностью к риску и необдуманным действиям, чаще попадают в ловушки мошенников (переходят по фишинговым ссылкам или раскрывают конфиденциальные данные под давлением). Также жертвы с такими чертами, как высокая доверчивость и отсутствие критического мышления, легче поддаются манипуляциям в схемах социальной инженерии (например, «романтическое» мошенничество или вишинг), а тревожность и заниженная самооценка могут приводить к пассивному виктимному поведению, когда жертва не сопротивляется давлению или не обращается за помощью из-за страха осуждения.

При анализе психологических портретов и различных видов преступлений в сфере информационно-коммуникационных технологий можно проследить, что данные виды эксплуатируют специфические психологические слабости. Так, фишинг и вишинг нацелены на людей с низкой осведомленностью о цифровых угрозах и высокой внушаемостью, а жертвы «романтического» мошенничества часто одиноки и обладают высокой потребностью в эмоциональной близости, что делает их уязвимыми к манипуляциям через сайты знакомств.

Необходимо отметить, что ряд когнитивных ошибок увеличивает риск процесса виктимизации. Например, эффект гипербдительности показывает излишнюю уверенность в своей безопасности («со мной этого не случится»), мешает распознавать угрозы [5]. Помимо этого, жертвы недооценивают вероятность негативного исхода, веря в «легкий заработок» в инвестиционных схемах. И, очевидно, невнимательность к деталям (к URL-адресам или грамматике в письмах) способствует успеху фишинга.

На наш взгляд, оценка виктимного потенциала различных групп населения в контексте ИКТ-преступлений – важная задача для профилактики и снижения рисков.

Виктимологический потенциал включает в себя состояние индивидуальной и групповой виктимизации в конкретный исторический момент, процесс виктимизации, виктимологическую стимуляцию, функциональный механизм соотношения «жертва – преступник» [6, с. 924].

Таким образом, можно выделить несколько ключевых факторов виктимности, такие как социально-демографические, поведенческие, психологические и технические:

1. Социально-демографические факторы:

– *возраст.* В группе риска, согласно исследованию Н. А. Кошкиной, Н. В. Каневой, Е. О. Тетерина, оказываются дети и подростки, поскольку обладают склонностью к рискованному поведению в соцсетях и доверчивостью к мошенническим предложениям, например в онлайн-играх [7, с. 47]. Однако, по мнению Павла Селезнева, декана факультета международных экономических отношений Финансового университета при Правительстве Российской Федерации, чаще всего жертвы – это люди среднего возраста, от 30 до 45 лет, со средним уровнем дохода. Пожилых людей тоже много, но не они основные пострадавшие;

– *уровень образования.* Люди с образованием ниже среднего в два раза чаще попадаются на фишинг из-за неумения анализировать URL-адреса или письма. Так, согласно опросу, проведенному Банком России в 2022 г. и отраженному в обзоре операций, совершенных без согласия клиентов финансовых организаций, по уровню образования жертвы распределились следующим образом: наибольшее количество жертв финансового мошенничества (48 %) составляют люди со средним профессиональным образованием, что свидетельствует о том, что эта группа наиболее уязвима, вероятно, из-за сочетания финансовой активности и недостаточных знаний о киберугрозах. При этом лица с высшим образованием, хотя и реже становятся жертвами (28,9 %), все же остаются в зоне риска, что опровергает стереотип об их полной защищенности, а наименьшая доля пострадавших среди людей с общим образованием (23,1 %) может объясняться их меньшей вовлеченностью в цифровые финансовые сервисы.

2. Поведенческие факторы:

– *активность в соцсетях.* Пользователи регулярно выкладывают фото из отпуска с геометками, подробно рассказывают о своем распорядке дня, публикуют данные о доходах или дорогих покупках, что вполне логично провоцирует злоумышленников на контакт с ними из-за «легкой добычи» информации. Все это приводит к осознанию того, что сегодня каждый является «открытой книгой» для рекламщиков, маркетологов, а также хакеров и киберпреступников, и поэтому насущной задачей для каждого пользователя является понимание рисков, связанных с присутствием в Сети, и контрмер, которые каждый может предпринять, чтобы сохранить собственную реальную и виртуальную идентичность [8, с. 327];

– *цифровая безопасность в повседневной деятельности:* например, отсутствие критичности при онлайн-знакомствах (так, подросток переводит деньги «новому другу» из игры, который просит «помощи на лечение»).

3. Психологические факторы:

– *виктимное мышление.* Жертва получает сообщение от несуществующей «службы безопасности банка» с требованием срочно перевести деньги на «безопасный счет» из-за «утечки данных». Вместо проверки информации (например, звонка в банк) человек сразу выполняет инструкции, так как подсознательно считает, что «эксперты знают лучше». Также установка жертвы «мне всегда не везет» или «я не разбираюсь в технологиях» снижает критичность мышления;

– *импульсивность.* Пользователь получает СМС: «Ваша карта заблокирована! Перейдите по ссылке для разблокировки». Вместо проверки номера отправителя или звонка в банк человек сразу кликает на фишинговую ссылку и вводит данные карты. Таким образом, мы видим, что импульсивные люди склонны поддаваться панике и действовать под давлением «дедлайнов», созданных мошенниками [5, с. 196].

4. Технические факторы:

– *утечки данных.* В России за 2024 год Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций фиксировала 135 случаев утечек баз данных, содержащих свыше 710 млн записей о гражданах.

Таким образом, виктимный потенциал населения в сфере ИКТ-преступлений является динамичным показателем, зависящим от различных факторов, поэтому снижение рисков требует комплексного подхода.

На наш взгляд, для снижения виктимного потенциала необходимы образовательные программы по безопасному поведению в цифровой среде для разных возрастных и социальных групп, технические меры защиты (искусственный интеллект, блокировка звонков, двухфакторная аутентификация и др.), а также пропаганда осознанного поведения в Интернете и критического восприятия подозрительных сообщений.

Рассмотрев оценку виктимологического потенциала в контексте ИКТ-преступлений и подчеркнув необходимость профилактических мер, логично обратить внимание на *социальную инженерию* как ключевой фактор виктимизации, поскольку именно манипуляция человеческим поведением, а не только технические уязвимости, лежит в основе большинства успешных атак в сфере информационно-коммуникационных технологий.

Социальная инженерия представляет собой комплекс методов, направленных на эксплуатацию психологических механизмов, таких как доверие, страх или авторитет, с целью обхода систем информационной безопасности. В условиях стремительного развития цифровых технологий и усложнения защитных механизмов изучение и предотвращение подобных угроз приобретает критическое значение.

Фишинг, претекстинг и техника «кью про кво» являются примерами методов социальной инженерии, которые, в отличие от технических уязвимостей, воздействуют на когнитивные искажения и уровень осведомленности пользователей.

Для углубленного понимания механизмов функционирования социальной инженерии целесообразно рассмотреть концептуальную модель ее воздействия. Данная модель представляет собой систематизированное представление о последовательности этапов, применяемых в социальной инженерии для достижения своих целей (рис.).

На первом этапе злоумышленниками осуществляется сбор и анализ релевантной информации, включая изучение социальных сетей, открытых источников и персональных данных жертвы, а также привлечение к процессу анализа лиц, обладающих экспертным знанием в данной области. После анализа определяется оптимальный метод воздействия, учитывающий особенности целевой аудитории, также оцениваются стратегии влияния, такие как обман, убеждение и манипуляция, для достижения максимального результата.

На втором этапе основное внимание уделяется формированию доверительных отношений с объектом воздействия. Для этого используются методы легкой беседы, затрагивающей общие темы, а также имитация авторитета для повышения уровня доверия. Создание повода для взаимодействия играет ключевую роль на данном этапе. Это может быть реализовано через различные предлоги, например предложение помощи, проведение опросов или обращение за технической поддержкой, что позволяет инициировать первый контакт и создать предпосылки для дальнейшего взаимодействия.

На третьем этапе применяются различные методы воздействия, направленные на достижение поставленной цели. Одним из таких методов является фишинг, который предполагает использование поддельных электронных писем или сообщений с целью побудить жертву выполнить определенные действия [9, с. 52]. Претекстинг представляет собой еще один эффективный метод, заключающийся в разыгрывании заранее подготовленного сценария [10, с. 95]. Использование эмоционального давления также является

Рис. Модель этапов, применяемых в социальной инженерии

распространенным методом воздействия. Оно может включать в себя манипуляции, направленные на вызов чувства жалости, желание помочь, невнимательность, а также незнание механизмов работы различных систем или ощущения срочности, что способствует более быстрому принятию решения объектом воздействия [11, с. 235].

На четвертом этапе осуществляется непосредственное достижение поставленной цели, которое может включать в себя получение конфиденциальной информации, денежных средств или доступа к определенным ресурсам, после чего необходимо закрепить достигнутый успех. Например, злоумышленник может добиться этого путем убеждения жертвы в законности проведенных действий или мягкого завершения общения, что позволяет избежать нежелательных последствий [12, с. 129].

На последнем этапе общение заканчивают – формально или неформально, в зависимости от ситуации. Также преступники предпринимают действия по сокрытию следов своей деятельности, удаляют конфиденциальную информацию и отзывают фишинговые письма. Кроме того, проводится анализ и обработка полученных данных, что может подразумевать их интеграцию в информационные системы или коммерческое использование на черном рынке, либо непосредственная реализация ранее задуманного плана.

Таким образом, социальная инженерия представляет собой метод манипуляции, основанный на психологии [13, с. 21, 23], а не на технических уязвимостях. Главная опасность заключается в том, что даже самые защищенные системы уязвимы, если человек по невнимательности или доверчивости раскроет данные. Поэтому, помимо технологической безопасности, критически важны осведомленность и здоровый скептицизм в любой ситуации, требующей передачи конфиденциальной информации.

Заключение

Разнообразие потенциальных жертв ставит перед нами сложную задачу. Невозможно вывести единый портрет, подходящий каждому пострадавшему от фишинга, взлома аккаунта или утечки персональных данных. Соответственно, необходимо понимать, что «жертва преступлений, совершаемых с использованием информационно-коммуникационных технологий» – это крайне гетерогенная группа, объединенная лишь фактом совершенного в отношении нее преступления в цифровой среде. Для более точного анализа и выделения характерных черт личности необходимо учитывать конкретный тип совершенного преступления, от которого пострадал человек.

Тем не менее проведенное исследование позволило выделить ключевые особенности личности жертвы преступлений в сфере информационно-коммуникационных технологий, а также определить факторы, способствующие повышенной виктимности.

Особое внимание в работе было уделено методам социальной инженерии, которые остаются одним из наиболее эффективных инструментов злоумышленников. Манипу-

лятивные техники, основанные на психологическом воздействии, демонстрируют, что даже технически подготовленные пользователи могут стать жертвами при должном уровне убеждения и эксплуатации человеческих слабостей. Это подчеркивает необходимость комплексного подхода к профилактике рассматриваемых преступлений, включающего не только технологические меры защиты, но и повышение осведомленности пользователей о тактиках социальной инженерии. Несмотря на полученные результаты, тема остается актуальной и требует дальнейшего изучения.

СПИСОК ИСТОЧНИКОВ

1. Суханова А. А. К вопросу об объеме и содержании понятия «жертва»: обзор теоретических позиций виктимологической науки // Вестник Челябинского государственного университета. Сер.: Право. 2020. Т. 5, № 1. С. 27–33. https://doi.org/ 10.24411/26188236202015105.

2. Фещенко П. Н. О возрастании негативных последствий «пассивной» виктимности в современной России // Виктимология. 2020. № 4 (26). С. 28–36.

3. Игнатова Е. С. Манипуляция эмоциональной безопасностью кибермошенниками с применением технологий социальной инженерии: case-study // Вестник Пермского университета. Философия. Психология. Социология. 2024. № 3. С. 374–390. https://doi.org/10.17072/2078-7898/2024-3-374-390.

4. Ильин И. С., Рязанова Е. Н. Виктимологическое предупреждение краж и мошенничеств, совершаемых бесконтактным способом // Закон и право. 2024. № 12. С. 208–214.

5. Власова Н. В., Буслаева Е. Л. Психологические особенности лиц, склонных к кибервиктимному поведению // Психология и право. 2022. Т. 12, № 2. С. 194–206. https://doi.org/10/17759/psylaw.2022120214.

6. Матусевич А. М., Кубышко Л. В. Психологические аспекты виктимности // Молодой ученый. 2014. № 8. С. 924–927.

7. Кошкина Н. А., Канева Н. В., Тетерин Е. О. Киберпреступность в подростковой среде: формы и способы профилактики // Международный журнал гуманитарных и естественных наук. 2023. № 8-1 (83). С. 46–50. https://doi.org/10.24412/2500-1000-2023-8-1-46-50.

8. Андреева М. Б. Покажи мне свой аккаунт, и я скажу тебе, кто ты. Про цифровую безопасность и «цифровой след» // Цифровое воспитание: реалии и перспективы : сб. материалов Междунар. науч.-практ. конф., Москва, 15 сент. 2022 г. / отв. ред. : Л. Ю. Максимова, Л. А. Григорович. М. : Негосударственное образовательное частное учреждение высшего образования «Московский институт психоанализа», 2022. С. 326–330.

9. Какорин И. А. Особенности фишинговых писем // Тенденции развития науки и образования. 2023. № 96-9. С. 52–55. https://doi.org/ 10.18411/trnio-04-2023-462.

10. Зотина Е. В. Претекстинг как прием социальной инженерии, используемый телефонными мошенниками: криминологический взгляд на проблему // Вестник Казанского юридического института МВД России. 2022. Т. 13, № 4 (50). С. 93–99. https://doi.org/10.37973/KUI.2022.55.63.012.

11. Бойко И. А., Стойчин К. Л. Проблема современных методов социальной инженерии // Безопасность информационного пространства – 2017 : XVI Всерос. науч.-практ. конф. студентов, аспирантов и молодых ученых, Екатеринбург, 12 дек. 2017 г. / Министерство образования и науки Российской Федерации, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина. Екатеринбург : Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, 2018. С. 234–238.

12. Сивчук Е. С. Социальная инженерия как способ мошенничества // Молодой ученый. 2020. № 41 (331). С. 128–130.

13. Ламинина О. Г. Возможности социальной инженерии в информационных технологиях // Гуманитарные, социально-экономические и общественные науки. 2017. № 2. С. 21–23.

REFERENCES

1. Sukhanova A. A. To the question about the volume and the content of the concept “victim”: a review of the theoretical positions of victimological science // Bulletin of Chelyabinsk State University. Series: Law. 2020. Vol. 5, no. 1. P. 27–33. https://doi.org/ 10.24411/26188236202015105. (In Russ.)

2. Feshchenko P. N. On the increasing negative consequences of “passive” victimization in modern Russia // Victimology. 2020. No. 4 (26). P. 28–36. (In Russ.)

3. Ignatova E. S. Manipulation of emotional security by cybercriminals using social engineering technologies: a case study // Perm University Herald. Philosophy. Psychology. Sociology. 2024. No. 3. P. 374–390. https://doi.org/10.17072/2078-7898/2024-3-374-390. (In Russ.)

4. Ilyin I. S., Ryazanova E. N. Victimological prevention of thefts and frauds committed by contactless means // Law and right. 2024. No. 12. P. 208–214. (In Russ.)

5. Vlasova N. V., Buslaeva E. L. Psychological features of individuals prone to cyber victimization // Psychology and law. 2022. Vol. 12, no. 2. P. 194–206. https://doi.org/10/17759/psylaw.2022120214. (In Russ.)

6. Matusevich A. M., Kubyshko L. V. Psychological aspects of victimization // Young scientist. 2014. No. 8. P. 924–927. (In Russ.)

7. Koshkina N. A., Kaneva N. V., Teterin E. O. Cybercrime in the teenage environment: forms and methods of prevention // International Journal of Humanities and Natural Sciences. 2023. No. 8-1 (83). P. 46–50. https://doi.org/10.24412/2500-1000-2023-8-1-46-50. (In Russ.)

8. Andreeva M. B. Show me your account and I’ll tell you who you are. About the digital safety and the digital footprint // Digital education: realities and prospects : proceedings of the International scientific and practical conference, Moscow, September 15, 2022 / ed. by L. Yu. Maksimova, L. A. Grigorovich. Moscow : Non-governmental educational private institution of higher education “Moscow Institute of Psychoanalysis”, 2022. P. 326–330. (In Russ.)

9. Kakorin I. A. Features of phishing letters // Trends in the development of science and education. 2023. No. 96-9. P. 52–55. https://doi.org/ 10.18411/trnio-04-2023-462. (In Russ.)

10. Zotina E. V. Pretexting as a social engineering technique used by telephone scammers: a criminological view of the problem // Bulletin of Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2022. Vol. 13, no. 4 (50). P. 93–99. https://doi.org/10.37973/KUI.2022.55.63.012 (In Russ.)

11. Boyko I. A., Stoichin K. L. The problem of modern methods of social engineering // Information space security – 2017 : the 16th all-Russian scientific and practical conference for students, postgraduates and young scientists, Yekaterinburg, December 12, 2017 / Ministry of Education and Science of the Russian Federation, Ural Federal University named after the first President of Russia B. N. Yeltsin. Yekaterinburg : Ural Federal University named after the first President of Russia B. N. Yeltsin, 2018. P. 234–238. (In Russ.)

12. Sivchuk E. S. Social engineering as a method of fraud // Young scientist. 2020. No. 41 (331). P. 128–130. (In Russ.)

13. Laminina O. G. Possibilities of social engineering in information technologies // Humanities, socio-economic and social sciences. 2017. No. 2. P. 21–23. (In Russ.)

Информация об авторе:
Голубева Л. А. – адъюнкт.

Information about the author:
Golubeva L. A. – adjunct.

Статья поступила в редакцию 26.07.2025; одобрена после рецензирования 10.09.2025; принята к публикации 19.03.2026.

The article was submitted 26.07.2025; approved after reviewing 10.09.2025; accepted for publication 19.03.2026.