ПСИХОЛОГИЧЕСКИЕ НАУКИ

https://doi.org/10.5281/zenodo.10390697
УДК 159.9

Беркович О. Е., Матрёшина Е. Б., Иванова Д. В.

Беркович Ольга Ефимовна, кандидат педагогических наук, доцент, ФГБОУ ВО «Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского», Россия, 603022, г. Нижний Новгород, пр. Гагарина, 23. E-mail: olgaberkovich@yandex.ru.
Матрёшина Евгения Борисовна, кандидат психологических наук, доцент, ФГБОУ ВО «Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского», Россия, 603022, г. Нижний Новгород, пр. Гагарина, 23. E-mail: evgenia_nno@mail.ru.
Иванова Дарья Вадимовна, практикующий юрист, Россия, 601352, Владимирская обл., г. Судогда, ул. Октябрьская, д. 91. E mail: darivnv@yandex.ru.

Психологические причины виктимного поведения жертвы мошеннических действий в интернет-пространстве

Аннотация. Данная статья посвящена психологическим причинам виктимного поведения жертвы информационно-телекоммуникационного мошенничества. Данная проблема обусловлена непрекращающимся развитием современных цифровых технологий, внедрением их в различные сферы жизнедеятельности общества и, как следствие, увеличением количества и вариаций киберпреступлений. В данной статье уделено внимание формам кибермошенничества, понятию жертвы мошеннических действий в интернет-пространстве, психологическим особенностям данной жертвы. В данной статье обосновывается наличие связей между виктимным поведением жертвы кибермошенничества и социально-психологическими факторами, такими как окружающая обстановка, наличие и поведение третьих лиц, состояние эмоционального возбуждения и т.д. Также в статье поднимается и рассматривается вопрос взаимосвязи виктимности и умственного развития личности, ведется речь об индивидуальных особенностях жертвы и их проявлении в кризисные моменты.
Ключевые слова: киберпреступление, кибермошенничество, жертва, цифровые технологии, интернет-пространство, психологические причины, виктимное поведение, информационно-телекоммуникационные технологии.

Berkovich O.E., Matreshina E.B., Ivanova D.V.

Berkovich Olga Efimovna, Associate Professor of the Department of Criminal Law and Process of the Faculty of Law Federal state Autonomous educational institution of higher professional education "National research Nizhny Novgorod state University named after N.I. Candidate of sciencenes

(pedagogics), Lobachevsky", Candidate of Pedagogical Sciences, Associate Professor, Russia, 603022, Nizhny Novgorod, Gagarin Ave., 23. E-mail: olgaberkovich@yandex.ru.
Matreshina Evgeniya Borisovna, Associate Professor of the Department of Criminal Law and Process of the Faculty of Law Federal state Autonomous educational institution of higher professional education "National research Nizhny Novgorod state University named after N.I. Lobachevsky" Candidate of Psychological Sciences, Russia, 603022, Nizhny Novgorod, Gagarin Ave., 23. E-mail: evgenia_nno@mail.ru.
Ivanova Daria Vadimovna, student, Faculty of Law "National research Nizhny Novgorod state University named after N.I. Lobachevsky», Russia, 603022, Nizhny Novgorod, Gagarin Ave., 23. E-mail: darivnv@yandex.ru.

Psychological causes of victim behavior of the victim of fraudulent actions in the Internet space

Abstract. This article is devoted to the psychological causes of victim behavior of the victim of information and telecommunication fraud. This problem is caused by the continuous development of modern digital technologies, their introduction into various spheres of society and, as a result, an increase in the number and variations of cybercrimes. This article focuses on the forms of cyberbullying, the concept of a victim of fraudulent actions in the Internet space, and the psychological characteristics of this victim. This article substantiates the existence of links between the victim behavior of the victim of cyberbullying and socio-psychological factors, such as the environment, the presence and behavior of third parties, the state of emotional arousal, etc. The article also raises and examines the issue of the relationship between victimhood and mental development of the individual, it is about the individual characteristics of the victim and their manifestation in crisis moments.
Key words: cybercrime, cyberbullying, victim, digital technologies, Internet space, psychological causes, victim behavior, information and telecommunication technologies.

Процесс внедрения современных цифровых технологий влечет не только рост их влияния на различные сферы жизнедеятельности общества, но и увеличение количества и вариаций киберпреступлений. Сегодня, когда обмен персональными данными и конфиденциальными сведениями может происходить через социальные сети, месседжеры и специальные банковские приложения, появляется все больше новых способов совершения противоправных деяний с использованием информационно-телекоммуникационных технологий.

Согласно данным Следственного комитета Российской Федерации, с 2013 г. уровень преступности в области цифровых технологий возрос более чем в 20 раз. Исходя из статистических данных, в 2021 г. каждое седьмое преступление совершалось с использованием IT-технологий или в киберпространстве [5]. За апрель и май 2023 г. было зарегистрировано 205200 преступлений в сфере компьютерной информации, что на четверть (25,3%) больше по сравнению с аналогичным периодом 2022 г. [3]. В целом количество киберпреступлений в России имеет устойчивую тенденцию к увеличению.

А.Л. Осипенко отмечал, что криминальный интерес преступников цифровой среды обращен к передовым направлениям развития технологий: разработкам в области анализа «Больших Данных», когнитивных вычислений и создания искусственного интеллекта, а также средствам скрытного информационного воздействия на психику людей с целью управления их поведением [9, с. 182]. Преступность ведет своеобразную технологическую гонку с правоохранительной системой, разрабатывая и интегрируя в свою деятельность но-

вые мошеннические схемы и методы совершения противоправных действий.

Основная цель мошенников в сфере информационных технологий заключается в извлечении незаконной выгоды. Достигается она путем обмана, манипуляций и принуждения пользователей раскрыть конфиденциальную информацию, предоставить доступ к защищенным системам, добровольно перевести денежные средства. Существует несколько основных форм кибермошенничества:

1. Социальная инженерия (вишинг) – способ мошенничества, реализующийся путем телефонной связи кибермошенников, разыгрывающих определенные социальные роли (сотрудник банка, представитель правоохранительных органов и т.д.), с потенциальными жертвами с целью заполучить конфиденциальные данные абонента или добиться осуществления им самостоятельных переводов денежных средств по реквизитам мошенников.

По данным Банка России в первом квартале 2023 г. выявлено 19608, а так же с использованием методов социальной инженерии, что на 69,94% больше среднего значения за 2022 г. Кроме того, наиболее распространенные мошеннические номера – мобильные телефонные номера, выявленное количество данных номеров за указанный период составило 87146 единиц [8].

2. Поддельные сайты (фишинг) – способ интернет-мошенничества, реализующийся с помощью различных схем и инструментов в сети Интернет – фишинговых сайтов, предлагающих товары и услуги, поддельных сайтов банков – с целью получения доступа к персональным или иным конфиденциальным данным пользователей (например, данным паролей банковских карт).

По данным Банка России, в первом квартале 2023 г. выявлено 1889 фишинговых атак, что на 10,27% больше среднего значения за 2022 г. Кроме того, в указанный период фиксируется резкое увеличение фишинговых сайтов – 5462 единицы, при среднем значении 1612 единиц в 2022 г. (увеличение составило 238,83%) [8].

3. DDOS-атаки (атаки типа «отказ в обслуживании») – способ интернет-мошенничества, направленный на создание помех или полную остановку работы веб-сайта или другого сетевого ресурса.

Таким атакам, как правило, подвергаются ресурсы государственных органов и организаций, ресурсы СМИ, образовательных учреждений, компаний, связанных с финансами, телекоммуникациями, здравоохранением и т.д. В первом квартале 2023 г. по данным Банка России было зарегистрировано 95 DDOS-атак [8].

Существуют и иные формы кибермошенничества. В частности, одной из схем мошеннических действий является оформление кредита в мобильном приложении [6]. Данная схема состоит в запугивании потенциальной жертвы недостоверной информацией – о работнике банка, предпринимающем попытки оформить кредит на клиента – и последующем оформлении обманным путем предодобренного кредита. В данном случае преступник преследует цель украсть кредитные средства клиента, а не собственные.

Еще одной изощренной мошеннической схемой, набравшей популярность во время пандемии, являются фейковые курьерские доставки [6]. В ходе данной схемы создаются объявления на популярных сайтах, с помощью которых происходит заманивание жертв мошенничества. При оформлении товара или услуги злоумышленники предоставляют жертве ссылку на поддельный сайт, таким образом, выманивая у нее данные банковской карты.

Осмысление масштабов проблем киберпреступности приводит к необходимости анализа психологических причин виктимного поведения личности при осуществлении мошеннических действий в интернет-пространстве. Стоит отметить, что определить психологические причины виктимного поведения не представляется возможным без понимания содержания понятия «жертва», иногда именно ее пове-

дение способствует реализации преступного умысла мошенника.

В.Е. Христенко считал верным следующее определение: жертва – это человек (сторона взаимодействия), который утратил значимые для него ценности в результате воздействия на него другого человека (стороной воздействия) [15, с. 247]. При этом «сторона воздействия» в качестве субъекта имеет потенциальный количественный выбор от одного конкретного человека до коалиции государств.

По мнению Л.В. Франка жертвой может являться человек или общность людей, которым прямо или косвенно причинен вред преступлением [14, с. 85]. В.П. Коновалов излагал противоположное мнение, согласно которому к жертвам преступления стоит относить только физических лиц. Аргументировалось это тем, что преступление, нанося вред определенной общности людей, в любом случае наносит вред каждому представителю этой общности [7, с. 6].

Существует точка зрения, в соответствии с которой основу определения понятия «жертва» составляет формулировка потерпевшего, установленная Уголовно-процессуальным кодексом РФ. Согласно ст. 6 потерпевший – физическое лицо, которому преступлением причинен физический, имущественный, моральный вред, а также юридическое лицо в случае причинения преступлением вреда его имуществу и деловой репутации [13]. В.И. Полубинский и А.Л. Ситковский считают, что понятие «жертва преступления» шире определения «потерпевший». Жертвой может выступать лицо, которому преступлением уже нанесен физический и моральный вред, имущественный ущерб, вне зависимости от того, имеет ли он статус потерпевшего или нет [11, с. 208].

Анализируя приведенные выше определения, можно сформулировать следующее понятие жертвы мошеннических действий в интернет-пространстве – активный пользователь или абонент, получивший моральный вред и (или) имущественный ущерб от противоправных действий, реализуемых посредством сети Интернет и (или) средств социальной инженерии, вне зависимости от наличия или отсутствия у него статуса потерпевшего.

Жертва киберпреступлений может характеризоваться совокупностью определенных психологических характеристик, которые делают совершение противоправного деяния возможным и даже способствуют реализации преступного умысла мошенников. К данным признакам могут относиться, в частности, легковерность, доверчивость, несообразительность, азартность и т.д. Анализ таких характеристик необходим как для расследования, так и для профилактики данного вида преступлений, предупреждения потенциальных информационно-телекоммуникационных угроз.

Г. Шнайдер писал, что пусть и не существует «прирожденных жертв», но приобретенные человеком физические, психические и социальные характеристики способны склонить его к превращению в жертву преступления [4, с. 8]. По его мнению, такими характеристиками могут выступать какие-либо физические или иные недостатки, неспособность к самозащите, внешняя или материальная привлекательность и т.д.

В процессе анализа психологических особенностей жертв И.Г. Малкина-Пых описывала определенный комплекс факторов, которые влияют на виктимность личности. В качестве базовых состояний выступили подавленность, тревога и печаль. Кроме того, для жертв преступлений характерны доверчивость, наивность и чувство сострадания, потребность в поддержке и помощи, ощущение безысходности и физическая вялость. На склонность личности оказаться жертвой противоправного деяния могут повлиять тяжелое материальное положение и желание обогатиться, черты алчности и бережливости, социальной дезадаптивности, эмоциональной лабильности, одиночества, агрессивности и т.д. [4, с. 277-286]

Кроме того, И.Г. Малкина-Пых выделяла определенные позиции поведения жертв [4, с. 206]:

– корыстное или провоцирующее;

– излишне доверчивое, некритичное, основанное на суеверии;

– положительное, т.е. не связанное с негативными мотивами или некритичностью потерпевшего;

– создавшее условия, позволившие преступнику продолжать преступную деятельность.

Согласно результатам исследования, проведенном О.Н. Первушиной и А.А. Федоровым, для усредненного личностного профиля жертвы (в контексте указанного исследования шла речь о жертвах вишинга) характерны следующие качества [10, с. 102]:

– более высокий уровень доверчивости, так как более доверчивые люди склонны принимать ложную информацию за истинную даже в случае существования фактов недостоверности;

– более высокий уровень доброжелательности, так как подобные люди в виду нездорового оптимизма надеются на аналогичные коммуникативные установки у других, а доброжелательностью партнера легко воспользоваться;

– менее высокий уровень эмоциональной стабильности, так как проблемы с эмоциональной реактивностью приводят к отсутствию у человека способности принимать разумные решения, рационально мыслить и эффективно справляться со стрессом;

– более высокий уровень внушаемости, так как люди, которым присуща внушаемость, характеризуются некритической податливостью и готовностью подчиняться воздействиям, противоречащим их убеждениям и интересам.

При анализе психологических характеристик жертв мошеннических действий в интернет-пространстве следует принимать во внимание, что индивидуальные особенности личности могут проявляться по-разному, ее поведение может быть не только неосторожным, но даже провокационным. Важно придавать значение социально-демографическим и социально-психологическим факторам, например, поведению третьих лиц, окружающей обстановке, конкретной жизненной ситуации и т.д., именно данные факторы являются основными критериями виктимности жертвы кибермошенничества.

Кроме того, стоит отметить, что уровень умственного развития и когнитивных способностей не оказывает влияние на виктимность жертв интернет-мошенничества. Данный факт подтверждают результаты совместного исследования нескольких американских университетов, в котором приняло участие 1220 человек [1, с. 864]. Авторы исследования также отметили, что виктимизация не имеет связи с возрастом, полом, самооценкой, здоровьем, отметив при этом высокую роль ситуационных факторов (нахождение в состоянии эмоционального возбуждения, была ли жертва одна в момент мошенничества и т.д.). В качестве второго определяющего фактора было названо отсутствие знаний о видах мошенничества или тактики, которые используются для обмана жертв.

Выделяют несколько основных психологических причин виктимного поведения жертв кибермошенничества [2]:

1. «Принцип взаимности» или «вынужденная задолженность»: человек может считать себя обязанным, когда мошенник делает что-то для него (например, рассказывает об услуге, предлагает реализовать ее и т.д.).

Так, эксклюзивное предложение инвестировать деньги может рассматриваться людьми с высоким уровнем доброжелательности как услуга, что вызывает желание ответить тем же: от продолжения выслушивания коммерческой инициативы до подписки на фиктивную схему мошенников.

2. Создание видимости надежности и законности мошеннических схем через

опыт большинства.

Преступник может приводить различные аргументы, чтобы склонить жертву пойти на поводу мошеннических схем. Например, это может быть статистика о количестве людей, которые подписались на финансовую схему. Результаты исследований показывают, если человек видит, что другие люди предпринимают какое-либо действие, он чувствует, что и ему можно сделать это действие. Это становится особенно актуальным, когда люди оказываются в сложной и двусмысленной ситуации, например, во время коммерческого предложения: если мошенник на другом конце телефона скажет, что 75% людей пошли на риск и инвестировали деньги, то человек с гораздо большей вероятностью склонится к действию, даже если в тайне будет сомневаться в правдивости данного утверждения.

3. Людям нравится представлять себя в качестве последовательных и вежливых, чем активно пользуются мошенники, заставляя совершать даже небольшие действия, которые затем приобретают более масштабный характер.

Например, просто задавая жертве тривиальные вопросы («как дела?» и др.), мошенник побуждает ее к самообману, заставляя поверить в искреннюю заинтересованность неизвестного на другом конце телефона. Кроме того, тривиальные вопросы в конечном итоге приводят к более личным, попыткам получить конфиденциальные данные жертвы.

4. Ввиду страха упустить «выгоду» или возможность, которая больше не представится, люди склонны принимать быстрые решения, превращающие их в жертв мошеннических схем.

Это становится особенно актуальным в сложной и двусмысленной ситуации, например, когда мошенники в попытках оказать давление говорят о действии их предложения в течение ограниченного времени.

Кроме того, указывается малая вероятность того, что описанных причин по отдельности будет достаточно, чтобы побудить потенциальную жертву к действиям, противоречащим ее интересам, но в совокупности они могут стать мощным инструментом для мошенника.

Анализируя особенности личности жертв противоправных посягательств в информационно-телекоммуникационной среде, Ф.С. Сафуанов и Н.В. Докучаева выделили комплекс индивидуально-психологических особенностей: беспокойство, неуверенность в себе, подверженность настроению, эмоциональная неустойчивость, неусидчивость, гневливость, определенные способы психологической защиты в стрессовых и психотравмирующих ситуациях (например, фокусировка на эмоциях, поиск социальной поддержки и т.д.) [12, с. 85].

Таким образом, в качестве психологических причин виктимного поведения лиц при осуществлении мошеннических действий в интернет-пространстве выступают как эмоциональный (низкий уровень контроля, неуверенность в себе и т.д.), так и коммуникативный компоненты личности (доверчивость, неумение дипломатично выстраивать социальное взаимодействие и т.д.). Кроме того, приоритетное значение имеет эмоциональная оценка ситуации потенциальной жертвой и уровень влияния на нее со стороны иных лиц.

СПИСОК ЛИТЕРАТУРЫ

1. DeLiema M., Deevy M., Lusardi A., Mitchell O., Financial Fraud Among Older Americans: Evidence and Implications // The Journals of Gerontology: S. B. V. 75, I. 4. 2020. P. 861–868.
2. Five psychological reasons why people fall for scams – and how to avoid them. URL: https:// theconversation.com/five-psychological-reasons-why-people-fall-for-scams-and-how-to-avoid-them-102421 (дата обращения: 15.10.2023)

3. В России за четыре месяца на четверть выросло количество киберпреступлений. URL: https://tass.ru/obschestvo/17880195 (дата обращения: 30.09.2023)
4. Малкина-Пых И.Г. Виктимология. Психология поведения жертвы. М.: Эксмо, 2010.
5. Интервью / ТАСС, К. Семеновская. URL: https://tass.ru/interviews/10461383?ysclid=lnijjm51nt67790294 (дата обращения: 30.09.2023)
6. Как защититься от кибермошенников – шесть основных схем обмана. URL: https://trends.rbc.ru/trends/industry/6027ef6c9a7947206e6aec96 (дата обращения: 30.09.2023)
7. Коновалов В.П. Изучение потерпевших от преступлений с целью совершенствования профилактики правонарушений / В.П. Коновалов. М.: Изд-во ВНИИ МВД СССР, 1982. 72 с.
8. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств за I квартал 2023 года. URL: https://cbr.ru/statistics/ib/review_1q_2023/ (дата обращения: 30.09.2023)
9. Осипенко, А.Л. Организованная преступная деятельность в киберпространстве: тенденции и противодействие // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2017. №4 (40). С. 181-188.
10. Первушина, О.Н., Фёдоров, А.А. Личностные особенности жертв телефонного мошенничества // Вопросы психологии. 2022. Т. 68. №3. С. 92-103.
11. Полубинский В.И. Теоретические и практические основы криминальной виктимологии / В.И. Полубинский, А.Л. Ситковский. М., 2006.
12. Сафуанов Ф.С., Докучаева Н.В. Особенности личности жертв противоправных посягательств и интернете // Электронный журнал «Психология и право». 2015. Том №5. №4. С. 80-93.
13. «Уголовно-процессуальный кодекс Российской Федерации» от 18.12.2001 № 174-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 03.10.2023)
14. Франк Л.В. Потерпевшие от преступления и проблемы советской виктимологии / Л.В. Франк. М., 1977. 237 с.
15. Христенко В.Е. Психология жертвы. Харьков: Консум, 2001. 256 с.

REFERENCES (TRANSLITERATED)

1. DeLiema M., Deevy M., Lusardi A., Mitchell O., Financial Fraud Among Older Americans: Evidence and Implications // The Journals of Gerontology: S. B. V. 75, I. 4. 2020. P. 861-868.
2. Five psychological reasons why people fall for scams – and how to avoid them. URL: https://theconversation.com/five-psychological-reasons-why-people-fall-for-scams-and-how-to-avoid-them-102421 (date of request: 10/15/2023)
3. In Russia, the number of cybercrimes has increased by a quarter in four months. URL: https://tass.ru/obschestvo/17880195 (date of application: 30.09.2023)
4. Malkina-Pykh I.G. Victimology. Psychology of victim behavior. Moscow: Eksmo, 2010.
5. Interview / TASS, K. Semenovskaya. URL: https://tass.ru/interviews/10461383?ysclid=lnijjm51nt67790294 (accessed: 30.09.2023)
6. How to protect yourself from cybercriminals – six basic deception schemes. URL: https://trends.rbc.ru/trends/industry/6027ef6c9a7947206e6aec96 (date of application: 30.09.2023)
7. Konovalov V.P. The study of victims of crimes in order to improve the prevention of offenses / V.P. Konovalov. M.: Publishing House of the Research Institute of the Ministry of Internal Affairs of the USSR, 1982. 72 p.
8. Review of reporting on information security incidents during money transfer for the first quarter of 2023. URL: https://cbr.ru/statistics/ib/review_1q_2023 / (date of appeal: 30.09.2023)
9. Osipenko, A.L. Organized criminal activity in cyberspace: trends and counteraction // Legal science and practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia. 2017. No.4 (40). pp. 181-188.
10. Pervushina, O.N., Fedorov, A.A. Personal characteristics of victims of telephone fraud // Questions of psychology. 2022. Vol. 68. No.3. pp. 92-103.
11. Polubinsky V.I. Theoretical and practical foundations of criminal victimology / V.I. Polubinsky, A.L. Sitkovsky. M., 2006.

12. Safuanov F.S., Dokuchaeva N.V. Personality characteristics of victims of unlawful attacks and the Internet // Electronic journal "Psychology and Law". 2015. Volume No. 5. No. 4. pp. 80-93.
13. "Criminal Procedure Code of the Russian Federation" dated 12/18/2001 No. 174-FZ. URL: https://www.consultant.ru/document/cons_doc_LAW_34481 / (date of address: 03.10.2023)
14. Frank L.V. Victims of crime and problems of Soviet victimology / L.V. Frank. M., 1977. 237 p.
15. Khristenko V.E. Psychology of the victim. Kharkiv: Consum, 2001. 256 p.

Для цитирования:
Беркович О.Е., Матрёшина Е.Б., Иванова Д.В. Психологические причины виктимного поведения жертвы мошеннических действий в интернет-пространстве // Гуманитарный научный вестник. 2023. №11. С. 115-122. URL: http:// naukavestnik.ru/doc/2023/11/Berkovich MatreshinaIvanova.pdf