Оригинальная статья / Original article

УДК 343.797

https://doi.org/10.21869/2223-1501-2024-14-2-107-118

Виктимологическая характеристика кибермошенничества

А. В. Москальков[1]✉

[1] Московский университет имени А. С. Грибоедова
ул. Новая Басманная, д. 35/1, г. Москва 105066, Российская Федерация

✉ e-mail: 11amo@list.ru

Резюме

Актуальность. *Уголовная статистика последних лет подтверждает значительный рост в России мошенничества, совершаемого с использованием информационно-телекоммуникационных технологий. При рассмотрении способов совершения кибермошенничества на основании изучения приговоров судов по уголовным делам, контент-анализа средств массовой информации дается его виктимологическая характеристика. Особое внимание обращается на личность потерпевшего от мошеннических действий, совершенных в сети Интернет, и факторы, увеличивающие риск становления жертвой таких преступлений.*

Целью исследования *является дополнение теории криминологии новым знанием о цифровой виктимности потерпевших от мошенничества, совершаемого с использованием информационно-телекоммуникационных технологий, для эффективного противодействия ему.*

Задачи*: на основе обвинительных приговоров судов, сообщений средств массовой информации дополнить виктимологическую характеристику кибермошенничества на основе анализа имеющихся и новых способов его совершения.*

Методология*. При написании работы применялись следующие общенаучные и частнонаучные методы познания: анализ, синтез, индукция и дедукция, статистический, документальный, формально-юридический, формально-логический, системный и прогностический.*

Результаты исследования *состоят в выявлении и описании виктимного поведения лиц, ставших жертвами кибермошенничества. Описаны факторы, повышающие степень виктимности потенциальных потерпевших. Полученные результаты могут быть использованы правоохранительными органами для разработки наиболее эффективных методов виктимологической профилактики рассматриваемого вида виртуальных преступлений.*

Вывод*. В силу специфичности способа совершения мошенничества (дистанционное) оно является исключением из разработанных виктимологией положений о потерпевшем от преступления. По этой причине пострадавшими от кибермошенников могут стать разные типы потенциальных жертв.*

Ключевые слова*: кибермошенничество; информационно-телекоммуникационные технологии; виктимность; цифровая виктимизация; кибервиктимизация; интернет.*

Конфликт интересов*: Автор декларирует отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.*

Для цитирования: Москальков А. В. Виктимологическая характеристика кибермошенничества // Известия Юго-Западного государственного университета. Серия: История и право. 2024. Т. 14, № 2. С. 107-118. https://doi.org/10.21869/2223-1501-2024-14-2-107-118.

Поступила в редакцию 04.03.2024 Принята к публикации 28.03.2024 Опубликована 27.04.2024

Victimological Characteristics of Cyberbullying

Artem V. Moskalkov[1] ✉

[1]Moscow University A. S. Griboedov
Novaya Basmannaya Str. 35/1, Moscow 105066, Russian Federation

✉ e-mail: kamenskiy.maxim@mail.ru

Abstract

Relevance. *Criminal statistics of recent years confirm a significant increase in fraud in Russia committed using information and telecommunication technologies. When considering the methods of committing cyberbullying on the basis of studying the sentences of criminal courts, content analysis of mass media, its victimological characteristics are given. Special attention is paid to the identity of the victim of fraudulent actions committed on the Internet and the factors that increase the risk of becoming a victim of such crimes.*

The purpose *of the study is to supplement the theory of criminology with new knowledge about the digital victimization of victims of fraud committed using information and telecommunication technologies in order to effectively counter it.*

Objectives: *on the basis of court convictions, media reports, to supplement the victimological characteristics of cyberbullying based on the analysis of existing and new ways of committing it.*

Methodology*. When writing the work, the following general scientific and private scientific methods of cognition were used: analysis, synthesis, induction and deduction, statistical, documentary, formal legal, formal logical, systemic and predictive.*

The results *of the study consist in identifying and describing the victimized behavior of persons who have become victims of cyberbullying. The factors that increase the degree of victimization of potential victims are described. The obtained results can be used by law enforcement agencies to develop the most effective methods of victimological prevention of this type of virtual crimes.*

Conclusion*. Due to the specificity of the method of committing fraud (remote) It is an exception to the provisions developed by victimology on the victim of a crime. For this reason, different types of potential victims can become victims of cybercriminals.*

Keywords*: cyberbullying; information and telecommunication technologies; victimization; digital victimization; cybervictimization; Internet.*

Conflict of interest: *The Author declare the absence of obvious and potential conflicts of interest related to the publication of this article.*

For citation: Moskalkov A. V. Victimological Characteristics of Cyberbullying. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo = Proceedings of the Southwest State University. Series: History and Law*. 2024; 14(2): 107–118. (In Russ.) https://doi.org/10.21869/2223-1501-2024-14-2-107-118

Received 04.03.2024 Accepted 28.03.2024 Published 27.04.2024

***

Введение

Социальное существование человека в современном обществе немыслимо без цифровизации. По верному замечанию Ю. Ю. Комлева, «за весьма короткое по историческим меркам время, благодаря компьютеризации и информационным технологиям, в центре которых Интернет, социум постмодерна приобрел зримые черты цифрового общества» [1, с. 33]. В структуре современной киберпреступности особое место занимают преступления против собственности, совершенные с использованием информационных технологий. По данным МВД РФ, количество мошенничеств с применением информационных технологий в 2022 г. по ст. 159 УК РФ «Мошенничество» составило 249 984; по ст. 159^3 УК РФ «Мошенничество с использованием электронных

средств платежа» – 7288; по ст. 159[6] УК РФ «Мошенничество в сфере компьютерной информации» – 334[1]. Очевидно, что стремительное развитие информационного общества порождает максимальные риски массовой виктимизации населения. Положение о том, что цифровые технологии, используемые в криминальных целях, не опосредованно, а напрямую обусловливают процесс виктимизации, доказывается в научной литературе. Криминологи справедливо пишут о том, что цифровизация породила новый вид виктимизации – цифровую [2, с. 148], и предлагают для введения в научный оборот новую терминологию (кибервиктимизация [3, с. 46] или кибервиктимность [4, с. 6]).

Тревожным трендом преступности с применением высоких технологий является многочисленность жертв, потерпевших от корыстных посягательств, что обусловливает необходимость активного поиска эффективных средств противодействия массовой виктимизации населения. А. Н. Игнатов, В. С. Соловьев справедливо указывают на то, что развитие информационных, коммуникационных и когнитивных технологий «меняет традиционные представления и подходы к исследованию виктимности и виктимизации, открывая перед криминологической наукой качественно новое исследовательское поле» [5, с. 63]. Исследованию вопросов виктимизации от мошенничества, ставшей следствием глобального развития цифровых технологий, посвящены труды Д. Ю. Дабаевой [6, с. 194], И. И. Евтушенко [7, с. 79], А. С. Камко [8, с. 141], Ю. Ю. Комлева, А. В. Майорова, Е. В. Никитина [9, с. 206], Д. В. Никулина [10, с. 390], С. А. Петрова [11, с. 50], Н. В. Сплавской [12, с. 17], О. А. Старостенко [13, с. 268], Д. В. Сынгаевского [14, с. 140] и др.

[1] Состояние преступности за январь-декабрь 2022 года // Министерство внутренних дел Рос. Федерации: сайт. URL: https://мвд.рф/reports/item/35396677/?ysclid=lofyqpnkjp374098658 (дата обращения: 22.01.2024).

Методология

В соответствии с темой исследования для достижения поставленной цели и решения задач использовались общенаучные и частнонаучные методы объективного познания действительности. С помощью методов анализа и синтеза, индукции и дедукции была определена сущность феномена виктимности потерпевших от кибермошенничества. Применение статистического и документального методов позволило обосновать актуальность исследования, изучить правоприменительную практику, интернет-источники, содержащие данные о мошеннических способах завладения чужой собственностью, а также научные позиции криминологов, обозначенные в публикациях по изучаемой тематике. Благодаря системному методу автор осуществил структурирование исследовательского материала. Формально-логический и формально-юридический методы явились основой построения исследовательского материала и аргументации авторских суждений, оказали содействие в осмыслении результатов и их описании. Прогностический метод был применен при определении перспектив дальнейшего развития этого вида виртуальных преступлений.

Проведенное исследование было основано на анализе приговоров, вынесенных по уголовным делам о мошенничестве, совершенном осужденными с использованием IT-технологий. Внимание автора было сосредоточено на личности жертвы корыстного киберпреступления. В общей сложности были изучены 85 приговоров, вступивших в законную силу за период с 2020 по 2023 г., текст которых был размещен на портале «Правосудие». Во внимание принимались и публикации средств массовой информации, содержащие данные о личности потерпевшего. По итогу был составлен

усредненный «портрет» жертвы мошенничества, совершенного с помощью интернет-технологий.

Результаты и их обсуждение

Описать виктимное поведение жертв кибермошенничества позволил анализ имеющихся «рабочих» и уже новых способов мошенничества, характеризующих его виктимологические аспекты. Тексты судебных приговоров и публикаций СМИ показывают, что наиболее распространёнными схемами мошенничества, совершаемого с использованием информационных технологий, являются:

1. *Мошенничество в отношении лиц, принадлежащих к одному профессиональному сообществу*. Мониторинг судебной практики показал, что жертвами серии мошеннических акций по новой криминальной схеме за последние полгода являлись преподаватели высших учебных заведений. В российской прессе опубликованы данные по фактам массовых рассылок сообщений в социальных сетях и мессенджерах (Vieber, «Телеграм», WhatsApp[1]) мошенниками. Они осуществляли переписку в чатах от имени руководства вузов, сотрудников Министерства образования РФ и Российской академии наук[2]. Так, с аккаунтов руководителей вузов, министра образования и науки В. Н. Фалькова и президента РАН Геннадия Красникова, похожих на оригинальные, с их фотографиями и логинами, жертве поступали сообщения или звонки с предупреждением о том, что с ней свяжутся «представители ФСБ РФ». Затем на связь выходил сообщник «ректора», представляясь сотрудником спецслужбы, который предлагал перевести деньги со своего банковского счета. Он якобы подвергся хакерской атаке со стороны украинцев, и чтобы не потерять деньги, нужен перевод на безопасный счет, на имя третьих лиц. При этом «секретный работник спецслужбы» требовал сохранить все в тайне, не сообщать об этом никому, даже близким, поскольку речь идет о государственной тайне. Мошенничество по такой схеме стало настолько распространенным, что Министерство образования и науки России на официальном сайте разместило соответствующее предупреждение[3].

Особое внимание Минобрнауки России обратило на то, что преступники используют технологии искусственного интеллекта для подмены голоса, а также чужие фотографии в мессенджерах. Кто из вузовского сообщества пострадал от мошеннического обмана? По сообщениям российских СМИ, потерпевшими стали профессор РАН, доктор юридических наук, которому позвонил «заместитель министра образования и науки РФ» (ущерб 6 млн руб.)[4]; доцент Уральского федерального университета, которому написал ректор с предупреждением о звонке «куратора из Минобрнауки». Он объявился и оформил на жертву кредит (ущерб 4 млн руб.)[5]; профессор консерватории в Саратове, получивший предупреждение от коллеги о звонке «сотрудника спецслужбы». Из-за угрозы перевода денег на финансирование противоправной деятельности с его банковских

[1] Принадлежит компании Meta, признанной экстремистской организацией и запрещенной на территории Российской Федерации.

[2] По нашим подсчетам, 65–85% звонков жертвам мошенничества поступает в мессенджерах «Вотсап», «Вайбер» и «Телеграм».

[3] Минобрнауки России предупредило о новой схеме телефонных мошенников // Гарант.ру: сайт. URL: https://www.garant.ru/news/165 (дата обращения: 19.01.2024).

[4] Юрист-ученый РАН отдал мошенникам более 6,6 млн рублей // Газета.ru: сайт. URL: https://www.gazeta.ru/business/news/2024/01/13/22104481.shtml?ysclid=ls0bhu0mma875915201 (дата обращения: 19.01.2024).

[5] Доктор наук объяснила, почему ученые и врачи верят финансовым мошенникам // RG.RU: сайт. URL: https://rg.ru/2023/09/20/reg-urfo/docenty-tozhe-platiat.html?ysclid=lssyyf2ai1684928218 (дата обращения: 19.01.2024).

счетов профессор перевел их на чужой счет (ущерб 2 млн 500 тыс. руб.). Как оказалось, аккаунт коллеги в мессенджере был взломан[1].

В числе обманутых мошенниками тем же способом оказались и депутаты Государственной Думы РФ, артисты. К примеру, депутату Государственной Думы Павлу Качкаеву написал в мессенджере «Телеграм» «зампред Госдумы Петр Толстой» (ущерб 500 тыс. руб.)[2], а актрисе МХТ имени А. П. Чехова Марии Зориной поступил звонок от «заместителя руководителя Департамента культуры г. Москвы» (ущерб 20 млн руб.)[3].

Аналогичная схема используется и в отношении врачей и медицинского персонала поликлиник и больниц. Им поступают звонки с подменных номеров в мессенджерах от имени заместителя министра здравоохранения РФ, главного врача, руководителя или заместителя руководителя департамента здравоохранения и др. Легенда здесь может меняться: например, преступники запугивают возбуждением уголовного дела по факту коррупции в больницах. «Целевой аудиторией» аферистов стали и учителя. Их данные опубликованы на официальных сайтах школ, где вместе с именами и фамилиями можно узнать сведения о возрасте, образовании и стаже работы. Парадоксально, но тотальная информатизация школ, поликлиник, больниц и вузов с обязательным информационным поводом (мероприятием, событием с упоминанием личных данных) на публичных порталах увеличила риски кибермошенничества. Она привела к тому, что поиск сведений злоумышленниками о потенциальных жертвах был существенно упрощен. Манипуляция ими при первичной «обработке» жертвы гарантирует криминальный «успех» по выманиванию денег или информации у нее.

Как отмечают специалисты, виктимность людей интеллектуального труда состоит в том, что ввиду высокого уровня ответственности они относятся к информации, поступившей от руководства, серьезно. К тому же расчет мошенников основан на том, что в больших государственных вузах много структурных подразделений, тысячи сотрудников и преподавателей, которые не всегда знают друг друга. Не каждого из них руководитель вуза знает в лицо, а тем более по имени и отчеству. У жертв мошенников нет личного телефона ректора, главного врача или их заместителей. Рабочие и организационные вопросы решаются посредством корпоративной e-mail, а потому вряд ли преподаватель или врач имеют немедленную возможность для того, чтобы уточнить о звонке из профильного министерства или департамента.

Ввиду того, что преподаватели являются публичными людьми (принимают участие в конференциях, в том числе на онлайн-платформах, пишут статьи с указанием своих данных (телефоны, адреса электронной почты), их персональные данные находятся в открытом доступе (в том числе включая биометрические (голос)) [15, с. 94]. Личные данные и контакты сотрудников вузов (ФИО, телефоны, e-mail) размещены на сайтах вузов. Зная их, можно идентифицировать человека в мессенджерах, найти привязанный к ним аккаунт.

2. *Мошенничество в сфере онлайн-торговли*. Еще одна схема мошенниче-

[1] Преподать урок: в ФСБ предупредили об атаках мошенников на учителей и врачей // Известия: сайт. URL: https://iz.ru/1593795/dmitrii-bulgakov/prepodat-urok-v-fsb-predupredili-ob-atakakh-moshennikov-na-uchitelei-i-vrachei (дата обращения: 19.01.2024).

[2] Бывшего мэра Уфы, депутата Госдумы Павла Качкаева мошенники развели на полмиллиона рублей // gtrk.tv: сайт. URL: https://gtrk.tv/novosti/338053-byvshego-mera-ufy-deputata-gosdumy-pavla-kachkaeva-moshenniki-razveli-polmilliona (дата обращения: 19.01.2024).

[3] Мошенники развели актрису МХТ на 20 млн рублей, заставив продать квартиру и машину // Life: сайт. URL: https://life.ru/p/1626284 (дата обращения: 19.01.2024).

ства в сети – это фейковые магазины, когда преступниками создается сайт с предложениями о продаже товаров по низкой цене или дефицитных товаров. По статистике, опубликованной МВД РФ, в 2022 г. россияне перевели злоумышленникам за покупку товаров в фальшивых онлайн-магазинах 13,5 млрд рублей, что на 39% больше, чем в предыдущем. Мошеннические сайты копируют оригинальные сайты официальных магазинов, сохраняя их дизайн и похожее название, покупают услуги продвижения в онлайн-сервисах, рекламу у блогеров, которые вызывают доверие клиентов. К примеру, 05.02.2024 г. корреспондент канала РЕН ТВ рассказал о десятках жертв мошенников из разных городов России. На поддельном сайте предлагалась дешевая бытовая техника по низким ценам. Покупатели оформляли доставку и переводили деньги «продавцам». Потерпевших не смутило то, что деньги требовалось перечислить по реквизитам общества с ограниченной ответственностью, зарегистрированного на предпринимателя О. А. Ильюшенко через ИНН, а заказ осуществлялся только по электронной почте. За пару недель работы «магазина» злоумышленниками причинен ущерб на несколько миллионов рублей. По данному факту возбуждены уголовные дела сразу в нескольких регионах страны. А между тем в сети появилась новая площадка по продаже дешевой бытовой техники, зарегистрированная на ту же предпринимательницу. О том, что магазин фейковый, подтверждает и то, что продаваемый товар был давно снят с производства или с продажи[1].

Подобные схемы применяются преступниками и на платформах бесплатных объявлений о продаже товаров. Так, в октябре 2023 г. по телеканалу «Санкт-Петербург» прошло информационное сообщение о задержании сотрудниками УВД по Санкт-Петербургу по борьбе с киберпреступлениями интернет-мошенников. Ими оказались девятнадцатилетние жители Петербурга и Воронежа. Их жертвами стали продавцы известных площадок объявлений, размещенных в сети Интернет. Выражая готовность купить товар, преступники предлагали его собственникам воспользоваться опцией «Безопасная сделка». Они направляли ссылку, кликая по которой жертва попадала на фишинговый сайт, где указывала банковские реквизиты и пароли. Мошенники похищали деньги, которые переводили на криптовалютные кошельки. В квартирах при проведении обысков были изъяты телефоны, ноутбуки, банковские и симкарты, а также около полумиллиона рублей. По данным фактам возбуждено уголовное дело по признакам преступлений, предусмотренных ст. 158, 159 и 159[3] УК РФ. Следствием установлено, что потерпевшими были пять жителей Санкт-Петербурга и Ленинградской области[2].

3. *Мошенничество в сфере услуг*. Распространенной в сети Интернет является афера с предлагаемыми услугами, среди которых всевозможные курсы и обучения у онлайн-коучей. Многомиллионные предложения об их покупке можно встретить в социальных сетях, в том числе запрещенных в России, на сайтах, площадках объявлений, рекламе у блогеров. Сюда относятся случаи мошеннических действий, выражаемых в «инфоцыганстве». К примеру, блогер-миллионник и автор бизнес-тренингов А. Шабутдинов обвиняется в восьми эпизодах мошенни-

[1] Фейковые интернет-магазины обманули россиян, «гнавшихся» за дешевой техникой // Ren.tv: сайт. URL: https://ren.tv/news/v-rossii/1187699-feikovye-internet-magaziny-obmanuli-rossiian-gnavshikhsia-za-deshevoi-tekhnikoi?ysclid= lstwg0mc5w144351536 (дата обращения: 19.01.2024).

[2] В Петербурге поймали кибермошенников, создавших фиктивные онлайн-магазины // RG.RU: сайт. URL: https://rg.ru/2021/04/06/reg-szfo/v-peterburge-zaderzhany-sozdateli-fiktivnyh-internet-magazinov.html?ysclid=lsuj1sk2p1973418296 (дата обращения: 19.01.2024).

чества в особо крупном размере[1]. Проблема приняла такой глобальный масштаб, что депутаты Государственной Думы РФ внесли законопроект, согласно которому бизнес-коучи обязаны возвращать деньги за некачественные образовательные или информационно-консультационные услуги. Поправки предлагается внести в закон о защите прав потребителей[2].

Высокий спрос у пользователей сети наблюдается и на цыганские предсказания, оккультные и психологические услуги, которые предоставляются в режиме онлайн, когда жертва переводит деньги «медийному» лицу – психологу или экстрасенсу, а по факту скрывающемуся за дипфейком или фейковой страницей мошеннику. На просторах интернета процветает и мошеннический «бизнес» по псевдолечению или целительству, когда аферист снимает в режиме онлайн «порчу» либо «излечивает от неизлечимого заболевания». Деньги за такие услуги могут переводиться на электронные кошельки, банковские карты или криптокошельки [16, с. 172]. Виктимными факторами, которые способствовали становлению жертвой мошеннического обмана, в таких случаях следует признавать нахождение потерпевшего в тяжелой жизненной ситуации. Как правило, обращение к гадалкам, магам, психологам, целителям связано с тяжелой болезнью самого потерпевшего либо его близких, а потому он становится более уязвимым и доверчивым. Этим состоянием жертвы и пользуются преступники, чтобы заполучить ее деньги или иное имущество.

Распространенной схемой мошеннического обмана является так называемый «развод» клиента с фейкового аккаунта или сайта, когда услуги проститутки предлагают мошенники. Они осуществляют переписку с заказчиком услуги, а после перевода денежных средств за секс-услугу телефон «девушки» блокируется [17, с. 753].

Еще одной криминальной схемой является размещение в сети Интернет объявлений об оказании услуг по выкупу автомобиля с последующей его передачей покупателю якобы с предоставлением рассрочки платежа под проценты. Так, Канавинский районный суд г. Нижнего Новгорода вынес обвинительный приговор Н., который предлагал услуги по выкупу автомобилей. Он заключал с потерпевшими договор «поставки» и после получения от них первоначального взноса денежным переводом скрывался. Действуя по этой схеме, мошенник получал дополнительно деньги и за оформление документов на автомобиль (постановка на регистрационный учет), установку дополнительного оборудования, транспортировку автомобиля к месту проживания покупателя – будущего владельца[3].

4. *Мошенничество, связанное с финансовой сферой*. Как известно, некоторые виды мошенничества криминологи называют интеллектуальным преступлением. «Высшим криминальным пилотажем» в мошенничестве считается создание в сети Интернет нелегальных букмекерских контор. Здесь продаются прогнозы событий (в том числе политических, в сфере экономики, влияющие, к примеру, на курс валюты), договорные матчи, обу-

[1] Восемь эпизодов в уголовном деле: что грозит блогеру Аязу Шабутдинову // Ren.tv: сайт. URL: https://ren.tv/news/v-rossii/1159163-chto-izvestno-o-zaderzhannom-blogere-aiaze-shabutdinove?ysclid=lsu0sn0ath537143718 (дата обращения: 19.01.2024).

[2] Госдума собирает отзывы на проект, обязывающий бизнес-коучей возвращать деньги за бесполезные тренинги // RG.RU: сайт. URL: https://rg.ru/2023/11/08/prodavcy-zhelanij.html?ysclid=lsty50n7yo410499349 (дата обращения: 19.01.2024).

[3] Приговор Канавинского районного суда г. Нижнего Новгорода от 08.11.2018 по уголовному делу № 1-461/2018 // Судебные и нормативные акты РФ: сайт. URL: https:// sudact.ru/regular/doc/S3jPFpUigAxU/?regular (дата обращения: 19.01.2024).

чающие вебинары, лотереи и ставки в казино. Преступниками гарантируется выигрыш в 200–300%, а для убедительности предъявляются доказательства «выигрыша» (чеки банкоматов, скриншоты и видеозаписи якобы перевода денег на карту). Мошенники сначала осуществляют «трафик» клиентов со всевозможных сайтов, из мессенджеров и социальных сетей, а затем дарят «беспроигрышные» стратегии [18, с. 43].

Сюда же относится вовлечение потерпевших в финансовые пирамиды, когда мошеннические действия в отношении собственности осуществляются дистанционно. Интернет изобилует предложениями вложиться в акции, отобранные лучшими финансовыми аналитиками, однако инвестировать следует только через «специальных брокеров», у которых есть секретные стратегии. К другим брокерам обращаться нельзя, потому что они берут большие комиссионные проценты. Та же схема обмана используется при предложении инвестировать в криптовалюту, сетевые магазины, майнинг и др. А. С. Кокорев и Я. В. Шавыкин при описании личностных особенностей жертв финансовых пирамид, повышающих их виктимность, называют такие, как дефицит системного мышления, неумение понимать причинно-следственные связи, в том числе финансово-экономического характера, что свойственно «поколению ЕГЭ». К ним же относится и циничность поколения лиц в возрасте 30–40 лет, цель которых получить вожделенный «пассивный» доход, в том числе и за счет обмана других участников пирамиды. Втянутыми в финансовые пирамиды являются и те пользователи сети Интернет, которые не понимают сути сетевого маркетинга, доверяют финансовой информации из виртуального пространства [19, с. 48]. Россиян обманывают и под предлогом благотворительности, онлайн-знакомствами, предложением удаленной работы (чаще всего на маркетплейсах) и др.

Очевидно, что мошенники анализируют новостные источники и используют полученную информацию для совершения преступлений. И если в начале специальной военной операции они «оказывали помощь» в оформлении гражданства чужих государств, банковских и симкарт, то позднее тактика сменилась на запугивание уголовной ответственностью за «финансирование ВСУ» и «уклонение от мобилизации». Следует прогнозировать появление очередной новой схемы мошенничества и новой группы потерпевших, в том числе по профессиональной принадлежности, однако точно определить, какое резонансное событие или факт общественной жизни станет катализатором новых криминальных сценариев, невозможно. Ведь они, сценарии, есть плод деятельности организованных групп, состоящих из коллективов психологов, разрабатывающих скрипты с конкретной задачей для злоумышленников, хакеров, способных распознать абонента мессенджеров, и др.

В подборке приговоров среди потерпевших от мошенничества встречались потерпевшие по одному и тому же виду мошенничества с различным социальным положением и уровнем образования (наличие ученой степени доктора наук и среднего образования). Как справедливо пишут исследователи, мошенничество является исключением из «виктимологических правил», а потому его жертвами могут стать разные типы потенциальных жертв [20, с. 39].

Выводы

Подводя итоги исследования, учитывая уголовную статистику и судебную практику, можно дать только усредненную, в общих чертах, характеристику жертвы мошенничества, совершенного в сети Интернет, потому что демографические показатели (пол, возраст), социальный и психологический статус, семейное положение, уровень образования, про-

фессиональная принадлежность будут разными в зависимости от вида мошенничества. В соответствии с ним можно выделить типы жертв, схожих по виктимологическим показателям.

По нашим наблюдениям, высокой степенью виктимности, *во-первых*, обладают люди с низкой компьютерной грамотностью, неосведомленные или недооценивающие опасность криминальных атак в Сети, неуверенные пользователи интернета и гаджетов, либо, напротив, уверенные в том, что мошенники не смогут убедить их перевести деньги (юристы, профессиональная деформация). *Во-вторых*, в ряде исследованных случаев на решение обратиться к мошенникам (гадалкам и экстрасенсам) повлиял низкий образовательный уровень, психологическая внушаемость человека, а также его нахождение в трудной жизненной ситуации (тяжелая болезнь, проблемы материального характера). *В-третьих*, потенциальными жертвами мошенничества традиционно являются дети (подростки), пользующиеся мобильными гаджетами и детскими банковскими картами, и лица пожилого возраста, более доверчивые, нежели представители других возрастных групп. *В-четвертых*, парадоксально, но именно высокая правовая грамотность, равно как правовая непросвещенность, оказывают влияние на становление человека жертвой мошенничества. *В-пятых*, повышают риск подвергнуться корыстному хищению собственности и психофизические свойства личности, позволяющие осуществлять манипуляцию поведением и сознанием человека.

Список литературы

1. Комлев Ю. Ю. Цифровизация, сетевизация общества постмодерна и развитие цифровой криминологии и девиантологии // Вестник Казанского юридического института МВД России. 2020. № 1. С. 31–40.

2. Майоров А. В. Влияет ли цифровизация на виктимизацию в современном обществе? // Виктимология. 2022. № 2. С. 148–156.

3. Жмуров Д. В. Кибержертва: решение проблемы терминологической неопределенности // Вестник Восточно-Сибирского института Министерства внутренних дел России. 2021. № 2 (97). С. 45–56.

4. Антонян Е. А., Клещина Е. Н. Кибервиктимность // Вестник Пермского института ФСИН России. 2019. № 3 (34). С. 5–10.

5. Игнатов А. Н., Соловьев В. С. Информационно-когнитивные технологии в механизме цифровой виктимизации // Вестник Казанского юридического института МВД России. 2023. № 1 (51). С. 59–66.

6. Дабаева Д. Ю. Виктимологическая характеристика мошенничества, совершаемого с использованием телекоммуникационного и компьютерного оборудования // Молодой ученый. 2022. № 47 (442). С. 193–195.

7. Евтушенко И. И. Виктимологическая защита жертв дистанционных хищений // Виктимология. 2023. № 1. С. 78–88.

8. Камко А. С. Портрет жертвы мошенничества в сфере телекоммуникационных технологий // Власть и управление на Востоке России. 2017. № 3(80). С. 139–144.

9. Никитин Е. В. Обеспечение виктимологической безопасности и профилактики преступлений с использованием информационных технологий // Виктимология. 2022. № 2. С. 204–212.

10. Никулин Д. В. Жертвы мошенничества // Аллея науки. 2017. № 1 (17). С. 387–393.

11. Петров С. А. Доверие как условие совершения мошенничеств // Уголовное право. 2015. № 4. С. 49–52.

12. Сплавская Н. В. Взаимодействие жертвы и преступника в процессе совершения мошенничества // Государство и право в XXI веке. 2017. № 3. С. 16–20.

13. Старостенко О. А. Виктимологическая характеристика мошенничества, совершаемого с использованием информационно-телекоммуникационных технологий // Гуманитарные, социально-экономические и общественные науки. 2020. № 5. С. 267–270.

14. Сынгаевский Д. В. Мошенничество в глобальной сети Интернет как объект виктимологического исследования // Современный юрист. 2013. № 4. С. 136–144.

15. Алихаджиева И. С. Криминологические риски персональных данных: основные тенденции и прогнозы // Известия Юго-Западного государственного университета. Серия: История и право. 2023. № 13(3). С. 90–101.

16. Салаев З. Р. К вопросу о способе мошенничества, связанного с оказанием оккультных и психологических услуг // Образование и право. 2019. № 5. С. 171–175.

17. Алихаджиева И. С., Меркурьев В. В. К криминологическому определению и классификации преступлений, связанных с проституцией // Всероссийский журнал Байкальского государственного университета экономики и права. 2016. Т. 10, № 4. С. 750–760.

18. Сафонов В. Н., Харченко О. В. Криминологическое исследование мошенничества в сфере компьютерной информации на примере деятельности интернет-букмекерских контор // Журнал правовых и экономических исследований. 2021. № 4. С. 39–50.

19. Кокорев А. С., Шавыкин Я. В. Направления повышения финансовой грамотности населения в части противодействия современным финансовым пирамидам // Культура и безопасность. 2022. № 1. С. 47–53.

20. Майоров А. В., Яременко Н. Е. Виктимологический аспект мошенничества // Виктимология. 2019. № 3 (21). С. 36–41.

References

1. Komlev Yu. Yu. Cifrovizaciya, setevizaciya obschestva postmoderna i razvitie cifrovoi kriminologii i deviantologii [Digitalization, networking of postmodern society and the development of digital criminology and deviantology]. *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii = Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia*, 2020, no. 1, pp. 31–40.

2. Majorov A. V. Vliyaet li cifrovizacii na viktimizaciyu v sovremennom obshchestve? [Does digitalization affect victimization in modern society?]. *Viktimologiya = Victimology,* 2022, no. 2, pp. 148–156.

3. Zhmurov D.V. Kiberzhertva: reshenie problemy terminologicheskoj neopredelennosti [Cyberwarfare: solving the problem of terminological uncertainty]. *Vestnik Vostochno-Sibirskogo instituta Ministerstva vnutrennih del Rossii = Bulletin of the East Siberian Institute of the Ministry of Internal Affairs of Russia,* 2021, no. 2 (97), pp. 45–56.

4. Antonyan E. A., Kleshchina E. N. Kiberviktimnost' [Cybervictimity]. *Vestnik Permskogo instituta FSIN Rossii = Bulletin of the Perm Institute of the Federal Penitentiary Service of Russia*, 2019, no. 3 (34), pp. 5–10.

5. Ignatov A. N., Solov'ev V. S. Informacionno-kognitivnye tehnologii v mehanizme cifrovoi viktimizacii [Information and Cognitive Technologies in the Mechanism of Digital Victimization]. *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii = Bulletin of the Kazan Law Institute of MIA of Russia*, 2023, no. 14(1), pp. 59–66.

6. Dabaeva D. Y. Viktimologicheskaya kharakteristika moshennichestva, sovershaemogo s ispol'zovaniem telekommunikacionnogo i kompyuternogo oborudovaniya [Victimological characteristics of fraud committed using telecommunications and computer equipment]. *Molodoi uchenyi = Young scientist, 2022,* no. 47 (442), pp. 193–195.

7. Evtushenko I. I. Viktimologicheskaya zashchita zhertv distancionnykh khishchenij [Victimoiogical protection victims of remote theft]. *Viktimologiya = Victimology*, 2023, no. 10 (1), pp. 78–88.

8. Kamko A. S. Portret jertvy moshennichestva v sfere telekommunikacionnykh tehnologii [Portrait of a victim of fraud in the field of telecommunication technologies]. *Vlast' i upravlenie na Vostoke Rossii = Power and management in the East of Russia*, 2017, no. 3(80), pp. 139–144.

9. Nikitin E. V. Obespechenie viktimologicheskoi bezopasnosti i profilaktiki prestuplenii s ispolzovaniem informacionnykh tehnologii [Ensuring victimological safety and crime prevention using information technologies]. *Viktimologiya = Victimology*, 2022, no. 2, pp. 204–212.

10. Nikulin D. V. Zhertvy moshennichestva [Victims of fraud]. *Alleya nauki = Alley of Science*, 2018, no. 1 (17), pp. 387–393.

11. Petrov S. A. Doverie kak uslovie sovershenіya moshennichestv [Trust as a condition for committing fraud]. *Ugolovnoe pravo = Criminal law*, 2015, no. 4, pp. 49–52.

12. Splavskaya N. V. Vzaimodeystvie zhertvy i prestupnika v protsesse sovershenіya moshennichestva [The interaction of the victim and the criminal in the process of committing fraud]. *Gosudarstvo i pravo v XXI veke = State and law in the XXI century*, 2017, no. 3, pp. 16–20.

13. Starostenko O. A. Viktimologicheskaya kharakteristika moshennichestva, sovershaemogo s ispol'zovaniem informacionno-telekommunikacionnykh tehnologii [Victimological characteristics of fraud committed using information and telecommunication technologies]. *Gumanitarnie, socialno-ekonomicheskie i obshchestvennye nauki = Humanities, socio-economic and social sciences*, 2020, no. 5, pp. 267–270.

14. Syngaevskii D. V. Moshennichestvo v global'noj seti Internet kak ob"ekt viktimologicheskogo issledovaniya [Fraud in the global Internet as an object of victimological research]. *Sovremennyi yurist = Modern lawyer*, 2013, no. 4, pp. 136–144.

15. Alikhadzhieva I. S. Kriminologicheskie riski personal'nykh dannykh: osnovnye tendencii i prognozy [Criminological risks of personal data: main trends and forecasts]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo = Proceedings of Southwest State University. Series: History and Law*, 2023, vol. 3, no. 13, pp. 90–101.

16. Salaev Z. R. K voprosu o sposobe moshennichestva, svyazannogo s okazaniem okkul'tnyh i psihologicheskih uslug [To the question of the method of fraud related to the provision of occult and psychological services]. *Obrazovanie i pravo = Education and law*, 2019, no. 5, pp. 171–175.

17. Alikhadzheva I. S., Merkurev V. V. K kriminologicheskomu opredeleniyu i klassifikacii prestuplenii, svyazannykh s prostituciei [To the criminological definition and classification of prostitution-related crimes]. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2016, vol. 10, no. 4, pp. 750–760.

18. Safonov V. N., Kharchenko O. V. Kriminologicheskoe issledovanie moshennichestva v sfere komp'uternoj informacii na primere deyatel'nosti internet-bukmekerskih kontor [Criminological study of fraud in the field of computer information on the example of the activities of Internet bookmakers]. *Zhurnal pravovyh i ekonomicheskih issledovanij = Journal of Legal and Economic Research*, 2021, no. 4, pp. 39–50.

19. Kokorev A. S., Shavykin Ya. V. Napravleniya povysheniya finansovoi gramotnosti naseleniya v chasti protivodeistviya sovremennym finansovym piramidam [Directions for improving financial literacy of the population in terms of countering modern financial pyramids]. *Kul'tura i bezopasnost' = Culture and security*, 2022, no. 1, pp. 47–53.

20. Maiorov A. V., Yaremenko N. E. Viktimologicheskii aspekt moshennichestva [Victimological aspect of fraud]. *Viktimologiya = Victimology*, 2019, no. 3 (21), pp. 36–41.

Информация об авторе / Information about the Author

Москальков Артем Владиславович, аспирант, Московский университет имени А. С. Грибоедова, г. Москва, Российская Федерация,
e-mail: 11amo@list.ru

Artem V. Moskalkov, Post-Graduate Student, Moscow University A. S. Griboedov, Moscow, Russian Federation,
e-mail: 11amo@list.ru