ISSN 2500-4255

Научная статья
УДК 343.988
EDN QFQHWL
DOI 10.17150/2500-4255.2022.16(4).463-472

КИБЕРЖЕРТВА: ОСОБЕННОСТИ КЛАССИФИКАЦИИ

Д.В. Жмуров
Байкальский государственный университет, г. Иркутск, Российская Федерация

Информация о статье

Дата поступления
6 апреля 2022 г.

Дата принятия в печать
31 августа 2022 г.

Дата онлайн-размещения
30 сентября 2022 г.

Ключевые слова

Кибервиктимизация; жертвы в Интернете; кибервиктимность; кибервиктимология; интернет-потерпевший; жертвы цифровых преступлений; кибержертва; личность потерпевшего в виртуальном пространстве

Аннотация. В настоящей статье представлен авторский подход к классификации кибержертв, т.е. потерпевших от разного рода правонарушений (уголовных, административных) в интернет-пространстве. Опираясь на исследования отечественных ученых и проведя собственный анализ, автор усматривает четыре типа жертв, среди которых: 1) нейтральная, не допускающая провокационного поведения и не способствующая совершению против нее правонарушений; 2) побуждающая, которая своим активным поведением провоцирует, дополнительно мотивирует причинителя (потенциального нарушителя) к дискриминационным действиям; 3) аккомодирующая — та, что создает благоприятные условия и облегчает исполнение преступного расчета (чрезмерно доверчивая, некритичная, неопытная, пассивная, ищущая выгоду, страдающая психическим расстройством, пожилая или малолетняя, одинокая); 4) противодействующая — подозрительная, оппозиционная, препятствующая осуществлению дискриминационных действий (неосновательно бдительная, тревожная, мнительная), действия которой в конечном итоге приводят к виктимизации. Для каждой из четырех базовых единиц классификации приведены дополнительные подгруппы (подмножества) потерпевших. Предложенная классификация дополняется пояснениями и практическими примерами, подробно раскрывающими особенности и виктимологические характеристики жертв. Также автором разработана ментальная схема, визуально отражающая упомянутую классификацию и делающая ее восприятие более понятным. Кроме того, в исследовании анализируются мотивы виктимного поведения в сети Интернет и предлагается описание некоторых наиболее распространенных внутренних побудительных причин поведения потерпевших.

Original article

A CYBERVICTIM: SPECIFICS OF CLASSIFICATION

Dmitry V. Zhmurov
Baikal State University, Irkutsk, the Russian Federation

Article info

Received
2022 April 6

Accepted
2022 August 31

Available online
2022 September 30

Keywords

Cybervictimization; victims on the Internet; cybervictimity; cybervictimology; Internet-victim; victims of digital crimes; cybervictim; personality of a victim in virtual space

Abstract. The article presents the author's approach to the classification of cybervictims, i.e. victims of various offences (criminal, administrative) on the Internet. Using the research of Russian scholars and his own analysis, the author singles out four types of victims, including: 1) neutral, not characterized by provocative behavior and not triggering crimes against themselves; 2) encouraging, actively provoking in their behavior and providing additional motivation for the actor (the potential offender) to commit discriminatory actions; 3) accommodating — creating favorable conditions and easing the implementation of a criminal intent (overly trusting, non-critical, inexperienced, passive, searching profit, suffering from a mental disorder, elderly or underage, single); 4) opposing — suspicious, opposing, obstructing discriminatory actions (overly vigilant, anxious, mistrustful), whose actions eventually result in victimization. The author presents additional subgroups (subsets) of victims for each of the four basic classification units. The classification is supplemented by interpretations and examples that thoroughly describe the specifics and victimological characteristics of victims. The author has also developed a mental scheme that visualizes the abovementioned classification and makes it easier to understand. Besides, the article presents an analysis of the motives of victim behavior on the Internet and provides a description of some most common internal driving factors for the victims' behavior.

Кибержертвы весьма непохожи друг на друга. Одни страдают из-за собственной беспечности или необдуманных поступков, другие — от пассивности и бездействия, третьи — по иным причинам.

Сегодня предложены разные классификации жертв (Т.В. Варчук и К.В. Вишневецкий [1], П.С. Дагель [2], П.А. Кабанов [3], Е.П. Ким и А.А. Михайличенко [4], Д.В. Ривман [5], В.А. Ту-

ляков [6], Л.В. Франк [7] и др.). Они опираются на многообразие виктимогенных качеств их обладателей, мотивы деятельности, несопоставимость моделей поведения и пр. При всем разнообразии подходов некоторые из этих схем нуждаются в дополнении, соответствующем реалиям современного «цифрового» общества.

В качестве отправной точки и основания классификации можно предложить *направленность влияния жертвы на активность правонарушителя*. Она рассматривается в четырех модальностях, соотносимых с базовыми типами потерпевших, среди которых выделяются:

– *нейтральная жертва* — жертва, не допускающая провокационного поведения и не способствующая совершению против нее преступлений (положительная, никого не затрагивающая). Не формирует виктимогенных предпосылок;

– *побуждающая жертва* — жертва, которая своим поведением провоцирует, дополнительно мотивирует нарушителя к дискриминационным действиям (агрессивная, активная, инициативная). Демонстрирует подстрекательское положительное или отрицательное поведение;

– *аккомодирующая жертва* — та, что создает благоприятные условия и облегчает исполнение преступного расчета (чрезмерно доверчивая, некритичная, неопытная, пассивная, искатель бесплатной выгоды, страдающая психическим расстройством, пожилая или малолетняя, одинокая). Своими личностными качествами упрощает исполнение криминального замысла;

– *противодействующая жертва* — подозрительная, оппозиционная, препятствующая осуществлению дискриминационных действий жертва (неосновательно бдительная, тревожная, мнительная). Пытается избежать виктимизации, но именно это стремление становится причиной злоупотреблений в ее отношении.

В более широком смысле указанные жертвы подразделяются на две большие группы:

– *объективно уязвимые*, т.е. подверженные правонарушениям и слабо защищенные от негативных деяний в силу причин, не зависящих от личности потерпевшего (*нейтральный тип*);

– *субъективно уязвимые* — обнаруживающие потенциал причинения противоправного вреда в результате действия личностных, психолого-поведенческих факторов (*побуждающий, аккомодирующий, противодействующий типы*).

Рассмотрим каждый из четырех названных типов отдельно.

Нейтральная жертва не является носителем виктимогенных качеств и атрибутов, при этом в силу стечения обстоятельств становится пострадавшей стороной. К таким кибержертвам относится несколько категорий лиц:

1. Лица, не совершающие неосмотрительных или опасных действий, но ставшие объектами атак в силу несовершенства используемого ими программного обеспечения. Преступники находят в нем уязвимости, оставленные создателями, и пытаются извлечь из этого выгоду. Пользователь фактически «платит» виктимизацией за технические ошибки третьих лиц. Известны ситуации, когда дискредитации подвергаются целые кластеры эксплуатантов Windows, Android и пр. Например, в 2022 г. пользователи операционной системы Windows были атакованы через ярлыки файлов и программ [8].

2. Лица, ставшие жертвами разглашения личной информации, переданной на ответственное хранение и похищенной у конечного держателя. Это потерпевшие, которые на законных основаниях передали юридическим лицам свои персональные данные (сведения о частной жизни, платежные идентификаторы), но те не смогли обеспечить конфиденциальность их хранения. Такие вбросы происходят нередко: в Сети то и дело публикуются утечки баз данных мобильных операторов, ГИБДД [9], иных государственных органов и пр. Один из подобных случаев произошел в 2022 г., когда сведения о 25 млн клиентах транспортной компании СДЭК оказались в открытом доступе [10].

3. Лица, потерпевшие от хищения криптографических валют, иных средств платежа, электронных ценных бумаг, делегированных на хранение профильным компаниям (электронным депозитариям, биржам, банкам, блокчейн-экосистемам и т.п.). Потеря активов в данном случае связана с неисполнением этими компаниями обязательств по их сбережению от недружественных действий сторонних лиц. Торговая площадка, к примеру, может быть взломана, а деньги ее участников списаны. Так произошло с криптовалютной биржей Coinbase, которая в 2021 г. не смогла сохранить средства более чем 6 тыс. клиентов, чьи учетные записи были взломаны. Для компрометации использовалась некая уязвимость, позволяющая обойти функцию двойной аутентификации посредством SMS [11].

4. Жертвы кибервмешательства в технико-социальные процессы или работу устройств, повлекшего за собой возникновение опасных

рисков. Пострадавшими могут оказаться пассажиры беспилотного транспорта или воздушного судна, управление которым перехвачено удаленно (в случаях кибертерроризма), или пациенты больниц, не получающие лечения из-за организационной неразберихи после атаки на сервер учреждения. Известен случай, когда в результате таких действий из строя было выведено медицинское оборудование. Произошло это во время операции на головном мозге 13-летней пациентки, что поставило под угрозу ее жизнь [12]. Сюда можно причислить и потерпевших от шпионажа с помощью домашних и гостиничных систем наблюдения, при котором злоумышленники получают приватный контент без ведома проживающих [13]. К указанным жертвам, помимо прочего, относятся граждане, пострадавшие от веерных отключений электроснабжения в результате взлома энергетических сетей, например в Иерусалиме, Ивано-Франковске и др. [14]. В аналогичном ключе обсуждаются вопросы компрометации систем управления и безопасности атомных станций, а именно возможные последствия таких действий для неопределенного круга людей.

Нейтральные жертвы могут формироваться в криминальных ситуациях алогично и непредсказуемо. К примеру, в белорусском«деле Захаревича» фигурировали такие объекты кибермести, как женщина, желавшая купить недвижимость у матери преступника, и продавец пластиковых окон, стоимость которых показалась «электронному террористу» завышенной[1]. При этом никаких виктимогенных качеств жертвы не демонстрировали.

Побуждающая жертва — лицо, которое своей активностью стимулирует потенциального нарушителя к криминальным действиям. Оно может усиливать его решимость, влиять на процесс развития криминальной мотивации, подталкивать к реагированию предосудительным образом. Действия жертвы при этом могут быть как нормативными (социально-положительными или нейтральными), так и девиантными (асоциальными, деструктивными, противоправными). Среди данной категории лиц выделяются:

1. Агрессивная жертва, создающая криминогенную ситуацию своими деструктивными действиями. Исследователями отмечается, что некоторые люди, проявляя излишнюю агрессивность и вызывающе напористое поведение, могут провоцировать преступления в отношении себя. Известно, например, что почти 24 % всех жертв преступлений провели детство в атмосфере семейных неурядиц, конфликтов и насилия. Пережитое ими способствует проявлению агрессивности и провокативного поведения во взрослой жизни, что нередко приводит к их виктимизации [15]. Для потерпевших, относящихся к типу агрессивной жертвы, в той или иной степени характерны культ физической силы, лживость, злопамятность, черствость, хитрость, агрессивность, жестокость, циничность, мстительность [16].

Очевидно, что агрессивная жертва в киберпространстве имеет свои специфические особенности.

Во-первых, это связано с вербализацией и релятивной природой агрессии в цифровой среде. Физическое насилие там почти невозможно. Поэтому агрессия может проявляться в форме: ругательств, оскорблений; сравнений с животными или частями тела и т.д.; нарочитого прерывания взаимодействия; посланий, призывов к действию; проклятий, злопожеланий; использования просторечной или специальной лексики с отрицательной окраской; риторических вопросов, за которыми скрывается угроза; открытых угроз; указаний на некомпетентность, непрофессионализм; различных вредительских действий [17].

Во-вторых, в основе механизма формирования жертвы и ее исходного агрессивного поведения лежит «феномен социального растормаживания» (дезингибиции), предполагающий расчет на анонимность Интернета, убежденность в том, что социальное наказание и неодобрение не настигнут агрессора-жертву, а следовательно, и более низкий уровень самоконтроля потенциальных потерпевших.

Агрессивные жертвы обычно имеют низкую самооценку и считают себя менее привлекательными или важными, чем другие [18]. Они чрезмерно беспокоятся и считают себя несчастнее других [там же]. Ряд исследователей отмечают, что агрессивные жертвы более депрессивны и имеют больше соматических симптомов, чем иные агрессоры и жертвы [19]. Также обнаружено, что агрессивные жертвы склонны приписывать свои неудачи внешним факторам, таким как «несчастье», «ситуация», «обстоятельства», что указывает на определенные трудности в принятии на себя ответственности [20].

[1] В Белоруссии задержан хакер-мститель, промышлявший «электронным терроризмом». URL: https://www.securitylab.ru/news/510575.php.

ISSN 2500-4255

В зарубежных источниках о кибербуллинге выделено четыре подтипа агрессивных жертв: традиционные агрессивные жертвы; агрессивные кибержертвы (допускающие косвенное и прямое физическое насилие по отношению к сверстникам, но дискриминируемые в виртуальной среде); киберагрессивные жертвы (пострадавшие от социальной изоляции в коллективе и пытающиеся выместить агрессию в Интернете путем распространения компрометирующих материалов); киберагрессивные кибержертвы (жестоко обращающиеся со сверстниками в Интернете в ответ на аналогичные поступки) [21].

2. Активная жертва, создающая криминогенную ситуацию своими неагрессивными действиями. Такие потерпевшие инициируют криминальные события неоднозначными поступками (провоцирующими и самопричиняющими). Традиционно они описываются как лица с более высокими, чем у агрессивных жертв, нравственными установками, достаточно образованные и имеющие ценности, не допускающие насилия.

Сюда относят следующие подкатегории (по Д.В. Ривману): сознательные подстрекатели (обращающиеся с просьбой о причинении вреда); неосторожные подстрекатели (явно не формулирующие такой просьбы, но провоцирующие причинителя); сознательные и неосторожные самопричинители (наносящие себе ущерб нарочно или непредумышленно).

К сознательным подстрекателям можно отнести тех, кто целенаправленно ищет и вступает в так называемые группы смерти для того, чтобы получать от кураторов задания, направленные в конечном счете на самоубийство[2]. Если потерпевший находит такого куратора и обращается к нему с соответствующей просьбой, можно сказать, что он подстрекает его к доведению до самоубийства, а именно склоняет к ассистированному суициду в форме квеста.

Среди активных жертв встречаются неосторожные самопричинители. Так, неоднократно фиксировались эпизоды самозаражения, нанесения вреда собственным компьютерам при разработке и тестировании вредоносного программного обеспечения. Например, создатель инфостилера Raccoon, проверяя его функции, случайно раскрыл информацию о своей личности [22], а киберпреступная группировка Patchwork при разработке трояна Ragnatela по ошибке заразила собственные машины [23].

3. Инициативная жертва, чье положительное поведение приводит к причинению ей вреда. Уровень правового сознания таких жертв выходит за рамки бытовых знаний, для нее свойственна высокая степень морально-этического, общекультурного развития [24]. Иногда ее поведение именуют *гиперсоциальным*.

Инициативность понимается как стремление приносить обществу пользу, а также как деятельность, мотивированная заботой о других (просоциальная активность). При этом выраженное и осознанное стремление делать добро каждый интерпретирует по-своему. Поэтому поступки, «добрые» и «полезные» в представлении одних людей, у других могут вызывать неоднозначную и даже негативную реакцию. Иногда такие действия встречают серьезный отпор, квалифицируемый даже по уголовным статьям. Подобные случаи не редкость. Так, к инициативным жертвам можно отнести активистов Общественной палаты РФ, чей электронный ресурс был атакован по мотивам мести после разоблачения на нем ряда фейков, связанных с голосованием в 2020 г. [25], или активистов защиты леса в Химках, сайт которых который подвергся DDOS-атаке в ответ на их общественную деятельность [26].

Характер инициатив может быть самым разнообразным — от общественно-политических актов до тактичного замечания нарушителю правил форума.

Аккомодирующая жертва — та, чьи личностные качества избавляют причинителя от затруднений и проблем в реализации преступных намерений. Вместо сдерживающих обстоятельств и трудностей в достижении цели злоумышленник получает максимально комфортную для себя жертву, заранее подготовленную к нужным манипуляциям.

В отличие от побуждающего типа данный субъект не влияет на формирование мотивации преступника (не выступает в качестве причины поведения), а является источником условий, способствующих опасному деянию. К таким потерпевшим относятся:

– чрезмерно доверчивые — недогадливые, склонные к излишнему, неоправданному простодушию и легковерию;

[2] «Порежу всю семью». Как куратор «группы смерти» склонял детей к суициду // Аргументы и факты. 2006. 20 июня. URL: https://aif.ru/society/web/porezhu_vsyu_semyu_kak_kurator_gruppy_smerti_sklonyal_detey_k_suicidu.

– некритичные — воспринимающие ситуацию без должной мысленной проработки, детального осознания возможных исходов и последствий;

– неопытные — не имеющие достаточных знаний и навыков, позволяющих избежать виктимизации в Интернете, неосведомленные;

– пассивные — не оказывающие противодействия и не вступающие в конфронтацию с преступником, склонные к проявлению зависимого и беспомощного поведения [27];

– рискованные (отчаянные, с низким самоконтролем) — совершают поступки с высокой вероятностью нанесения себе ущерба, а также с преобладающим стремлением к получению острых ощущений, толерантные к риску;

– импульсивные — действующие под влиянием внезапных побуждений, зачастую вызванных кратковременными аффектами. В исследовании «Ограничение мошенничеств в телемаркетинге» установлено, что жертвы инвестиционного обмана склонны к спонтанным покупкам, а жертвы лотерей никогда или почти никогда не планируют будущие покупки [28];

– корыстолюбивые — алчные, жадные к наживе, легким деньгам, нетрудовому обогащению;

– психически неполноценные — страдающие психическими дефектами, повышающими риск виктимизации и непонимание актуальной коммуникативной ситуации;

– возрастные (пожилые или малолетние) — относящиеся к такому возрасту, когда спектр накопленных компетенций не гарантирует безопасность в виртуальных средах;

– фрустрированные (одинокие, субъективно несчастные, депривированные) — находящиеся в состоянии хронического неудовлетворения потребностей, желающие преодолеть эту ситуацию, проявляющие склонность к выражению неудовлетворенности жизнью [27].

Наличие тех или иных характеристик не обязательно является взаимоисключающим. У одного и того же потерпевшего они могут мультиплицироваться и сосуществовать в единой структуре личности.

Аккомодирующие жертвы терпят ущерб от разных правонарушений. Доверчивые попадают в ловушку методов социальной инженерии, когда ими манипулируют, выдавая себя за полицейских, работодателей, социальных работников и т.п. Корыстолюбивых застают врасплох, предлагая выгодные вложения, большие скидки и высокие заработки. Одинокие и несчастные могут стать жертвами брачных аферистов или «новых друзей» из социальных сетей. Рискованные и некритичные не обращают внимание на возможные риски своего поведения: вступают в интимные отношения, используют «пиратский» софт, забывают защищать информацию.

Противодействующая жертва — лицо, которое неэффективно сопротивляется возможным угрозам со стороны киберпреступников, форсируя собственную виктимизацию.

Мотив избегания виктимизации является одним из важнейших и ведущих в интернет-коммуникации. Исследование компании Ipsos в 28 странах (в том числе в России) показало, что взлом с целью мошенничества или шпионажа назван главным страхом абсолютного большинство респондентов — 75 %. Страх стать жертвой киберпреступников оказался весомее угроз ядерной или химической атаки, по поводу которых высказали опасения 68 % участников опроса [29]. Именно эти фобии злоумышленники обратили в свою пользу и успешно их эксплуатируют.

Наиболее известным примером являются случаи фишинга, когда мошенники представляются службой безопасности банка и похищают деньги клиента под видом профессиональной помощи. Сначала его запугивают, рассказывая, что кто-то снимает деньги со счета, затем успокаивают, гарантируя защиту, а в итоге путем разных уловок получают необходимую платежную информацию. Таким образом, противодействуя мнимым преступникам, потерпевший передает все данные в руки преступников настоящих.

Другим примером использования мотивов противодействия является обман при скачивании квазиполезных программ. Это группа приложений с разными декларируемыми задачами: одни защищают компьютер от вирусов, вторые оптимизируют его работу, третьи призваны сделать сетевой серфинг более безопасным и т.п. Пользователь, устанавливая эти продукты, считает, что заблаговременно защищает и ограждает себя от опасностей. Но на деле такие программы оказываются вредоносными. Это могут быть фальшивые антивирусы (псевдоантивирусы), представляющие разновидность троянских программ. Они имеют собственные наименования или маскируются под настоящие утилиты (например, Security Essentials 2010 вместо Microsoft Security Essentials или AntiVirus XP 2008 вместо Norton AntiVirus) [30]. Сюда же относятся программы оптимизации и различного рода тулбар-ассистенты, которые могут «подсовывать» рекла-

му, обеспечивать скрытые переходы на нужные хакерам сайты, навязывать покупки и т.д.

При описании противодействующих жертв нельзя обойти вниманием такое явление, как фальшивые интернет-центры защиты прав потерпевших. Своей целью они объявляют «поддержку» обманутых вкладчиков (дольщиков, инвесторов, пайщиков). В работе ориентируются на противодействующих жертв — тех, у кого после криминального инцидента не опустились руки и кто готов дальше бороться за свои права. Особый интерес представляют желающие компенсировать убытки, вернуть вклады или наказать виновных. Им предлагаются услуги подобного рода за немалую плату. По сути, это повторное мошенничество, когда оболваненный человек еще раз платит мошенникам. В рекламе они стараются использовать официальные названия, например «Комитет по защите акционеров», «Центр по защите прав обманутых вкладчиков». Часто ссылки в их сообщениях ведут на фишинговые сайты. Там людей убеждают, что им положены крупные суммы компенсации — нужно лишь оплатить юридические услуги. Но как только клиент вводит данные карты, преступники получают доступ к счету и похищают его содержимое [31]. Только один такой центр способен причинить ущерб на сумму более 100 млн р. [32].

Похожей формой обмана является история с выплатой компенсации после утечки данных. Например, пользователь получает письмо из «Фонда защиты персональных данных», созданного «Американской торговой комиссией», в котором сообщается, что ему положено возмещение за раскрытие его персональной информации. Уверенный в собственной правоте и восстановленной справедливости, он заполняет анкету на солидную выплату в несколько тысяч долларов. Все, что требуется для получения этой суммы, — американский номер соцстрахования (SSN), а купить его можно за девять с небольшим долларов на «специальном» сайте-фальшивке [33]. Этот случай наглядно подтверждает тот факт, что поствиктимное поведение жертвы, мотивированное компенсаторными побуждениями, «культурой отмены» преступления, может быть использовано для ее повторной дискредитации.

Итак, всех противодействующих жертв можно разделить на несколько подтипов:

– жертвы отмены (пытаются изменить или минимизировать наступившие последствия криминального акта; осуществляют поствиктимное поведение, опасное для них с точки зрения ревиктимизации);

– жертвы превенции (стараются заранее обезопасить себя от преступных посягательств, но своими неумелыми и некомпетентными действиями приводят к обратному).

– жертвы оппозиции (в случае уже осуществленного в их отношении посягательства своими неэффективным сопротивлением вызывают еще больший ущерб от виктимизации).

Описанная выше классификация кибержертв графически представлена в виде ментальной карты (рис.).

Что касается мотивации жертв, то ее можно определить как совокупность побуждений, которые в своем единстве формируют виктимное поведение. Детально раскрыть особенности мотивации позволяют рассмотренные выше типы потерпевших.

Очевидно, что мотивация жертв в Интернете зависит от намерений и потребностей потерпевшего лица. Ниже приведены некоторые общие мотивы поведения кибержертв. Выделяются:

– экономические мотивы (риск виктимизации во многом связан со стремлением к финансовой выгоде и материальному благополучию);

– мотивы аффилиации (тяга к сопричастности, желание обрести близкого человека, испытать любовь и дружбу, установить и поддерживать связи с другими людьми);

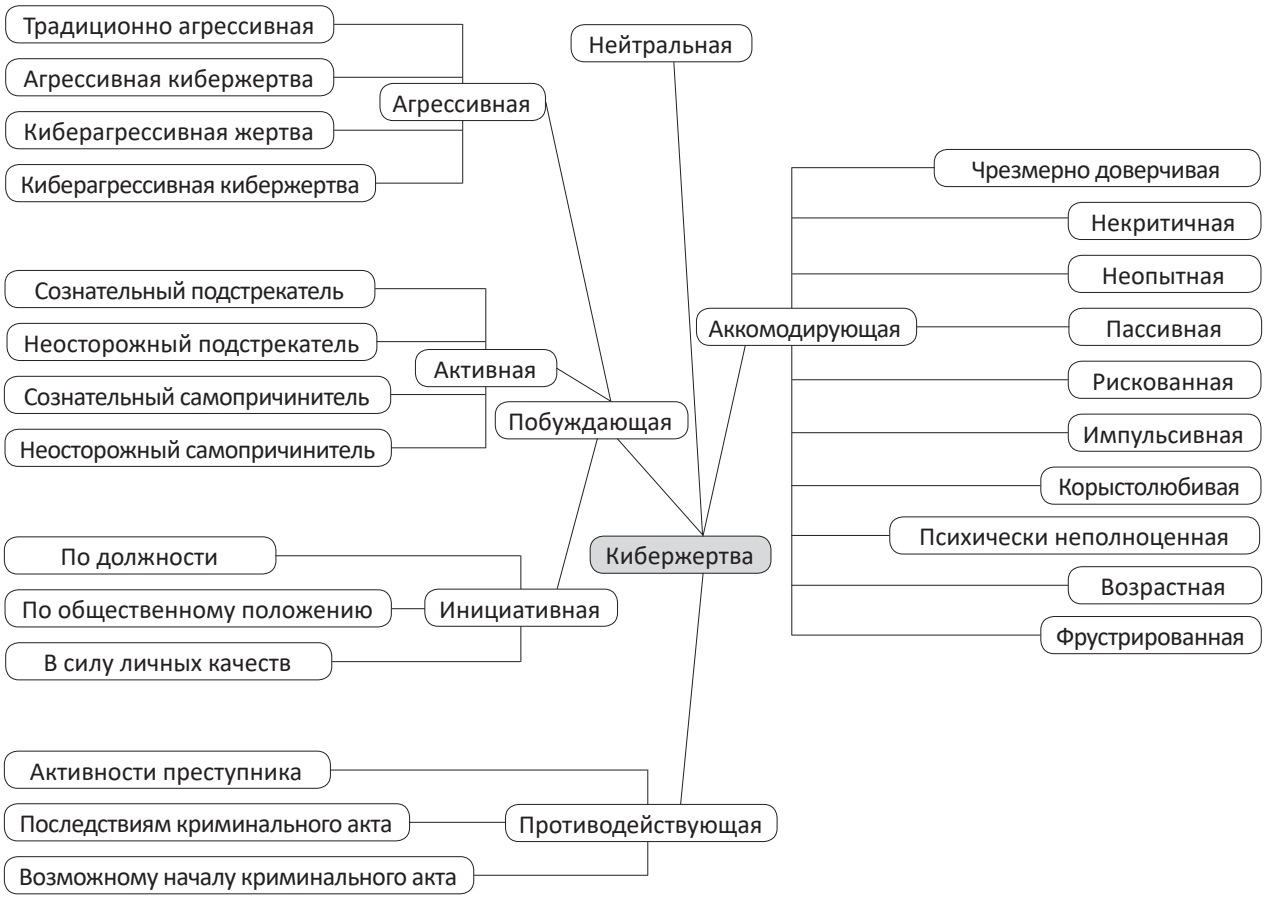
– сексуальные мотивы (стремление удовлетворить сексуальные потребности);

– политические мотивы (активность, связанная с осуществлением и приобретением власти, борьбой за нее, отстаиванием той или иной политической позиции);

– мотивы развлечения (побуждение к получению несексуального удовольствия различными способами — через общение на форумах, веселое времяпрепровождение, некритичное потребление цифрового контента, удовлетворение любопытства интереса за счет перехода по ссылкам);

– мотивы достижения (получение новых компетенций, обучение хакерским навыкам, профессиональный рост, трудоустройство, креативная и творческая деятельность, постинг, блоггерство, репостинг и записи на «стене» как суррогаты остроумия и мудрости);

– просоциальные мотивы, связанные с реализацией чувства долга перед обществом и нравственными обязанностями;



Классификация жертв в Интернете
Classification of victims on the Internet

– мотивы избегания, которые выражаются в склонности остерегаться ущерба, желании обезопасить себя;

– мотивы самоутверждения, как результат стремления к достижению и поддержанию определенного социального статуса;

– эмоциональные мотиваторы, связанные с виктимогенным проявлением субъективных переживаний в интернет-коммуникации (например, ненависть, гнев, мотивы мести, страхи).

Итак, кибержертвы далеко не идентичны. Несмотря на это, с определенными оговорками их множество можно свести к четырем основным классам: нейтральным, побуждающим, аккомодирующим и противодействующим жертвам. Настоящая классификация, вероятно, в чем-то справедлива и для классической виктимологии, поскольку не содержит в себе указаний на жертв, формирующихся только в киберпространстве, т.е. исключительно виртуальных.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Варчук Т.В. Виктимология : учеб. пособие / Т.В. Варчук, К.В. Вишневский. — Москва : Юнити-Дана, 2008. — 191 с.

2. Дагель П.С. «Вина потерпевшего» в уголовном праве / П.С. Дагель // Советская юстиция. — 1967. — № 6. — С. 10–11.

3. Кабанов П.А. Криминологическая классификация жертв политических преступлений в современной российской криминальной политической виктимологии / П.А. Кабанов. — EDN KFQFTJ // Юридическое образование и наука. — 2007. — № 4. — С. 24–27.

4. Ким Е.П. Виктимология: проблемы теории и практики : учеб.-метод. пособие / Е.П. Ким, А.А. Михайличенко. — Хабаровск, 2004. — 52 с.

5. Ривман Д.В. Криминальная виктимология / Д.В. Ривман. — Санкт-Петербург : Питер, 2002. — 304 с.

6. Туляков В.А. Виктимология. Социальные и криминологические проблемы / В.А. Туляков. — Одесса : Юридична література, 2000. — 336 с.

7. Элькинд П.С. Франк Л.В. Потерпевшие от преступления и проблемы советской виктимологии. Душанбе, «Ирфон», 1977, 237 с. / П.С. Элькинд, В.В. Вандышев. — EDN UCCMMV // Известия высших учебных заведений. Правоведение. — 1978. — № 4. — С. 117–118.

8. Ставицкий А. Пользователей Windows атаковали через ярлыки / А. Ставицкий // Lenta.ru. — URL: https://lenta.ru/news/2022/04/27/link.

9. Ломакин Б. Мошенники получили доступ к базе ГИБДД. Они могут красть машины и присылать фейковые штрафы / Б. Ломакин, Ф. Горин // 360tv.ru. — URL: https://360tv.ru/news/tekst/dostup-k-baze-gibdd.

10. Ясакова Е. В Сеть потенциально попали данные 25 млн клиентов СДЭК / Е. Ясакова // РБК. — URL: https://www.rbc.ru/technology_and_media/15/07/2022/62d022d09a794711851de88dd.

11. Stimolo S. Coinbase Reveals Phishing Attack, 6000 Users Robbed / S. Stimolo // The Criptonomist. — URL: https://en.cryptonomist.ch/2021/10/05/coinbase-phishing-attack-6000-users-robbed.

12. Левкович А. Хакеры совершили атаку на центр нейрохирургии во время операции ребенку / А. Левкович // Vademecum. — URL: https://clck.ru/sXmxG.

13. Куприянов С. «Русские хакеры» шпионили за постояльцами отелей с помощью эксплоита АНБ США / С. Куприянов // Технологии будущего. — URL: http://alterprogs.ru/russkie-khakery-shpionili-za-postoyal.html.

14. Котерадзе С. Кибератаки «повзрослели». Хакеры начали отключать свет в городах / С. Котерадзе // Eadaili. — URL: https://eadaily.com/ru/news/2016/02/02/kiberataki-povzrosleli-hakery-nachali-otklyuchat-svet-v-gorodah.

15. Сидоренко Э.Л. Виктимологическая провокация в уголовном праве России : учеб. пособие / Э.Л. Сидоренко. — Ставрополь : Изд-во Ставропол. гос. ун-та, 2005. — 126 с.

16. Артемьев Н.С. Криминологическое исследование поведения потерпевших в насильственных преступлениях в сфере семейно-бытовых отношений / Н.С. Артемьев. — EDN YUJQWJ // Человек: преступление и наказание. — 2018. — Т. 26, № 1. — С. 22–28.

17. Батурин А. Агрессия в интернете: методы противостояния / А. Батурин // RedKrab. — URL: https://redkrab.ru/blog/marketing/agressiya-v-internete-metodi-protivostoyaniya.

18. O'Moore M. Self-esteem and its Relationship to Bullying Behavior / M. O'Moore, C. Kirkham // Aggressive Behavior. — 2001. — № 27. — P. 269–283.

19. Psychosocial Correlates in Bullying and Victimization: The Relationship Between Depression, Anxiety, and Bully/Victim Status / S.M. Swearer, S.Y. Song, P.T. Cary [et al.]. — DOI 10.1300/J135v02n02_07 // Journal of Emotional Abuse. — 2001. — № 2. — P. 95–121.

20. Georgiou S.N. Victims and Bully — Victims. Psychosocial Profiles and Attribution Styles / S.N. Georgiou, P. Stavrinides // School Psychology International. — 2008. — Vol. 29, iss. 5. — P. 574–589.

21. Cuadrado-Gordillo I. Cyberspace as a Generator of Changes in the Aggressive-Victim Role / I. Cuadrado-Gordillo, I. Antelo. — DOI 10.1016/j.chb.2014.03.070 // Computers in Human Behavior. — 2014. — № 36. — P. 225–233.

22. Нефедова М. Разработчик малвари Racoon заразил свою систему и слил собственные данные / М. Нефедова // Хакер. — 2021. — № 8. — URL: https://xakep.ru/2021/08/17/raccoon-leak.

23. Иванов О. APT-группа Patchwork заразила свои компьютеры и выдала нюансы операций / О. Иванов // Anti-Malware. — URL: https://clck.ru/u4WQ3.

24. Артемьев Н.С. Вопросы типологии жертв преступлений, совершаемых в сфере семейно-бытовых отношений / Н.С. Артемьев, Е.Г. Полищук. — EDN NXMCRH // Вестник Рязанского государственного университета им. С.А. Есенина. — 2007. — № 17. — С. 82–90.

25. Никонов Н. Сайт Общественной палаты России и проект «Фейкам.нет» подверглись DDoS-атаке / Н. Никонов // Life. — URL: https://life.ru/p/1332092.

26. Гурская Н. Сайт защитников Химкинского леса атаковали хакеры / Н. Гурская // The Epoch Times. — URL: https://www.epochtimes.ru/content/view/80124/3.

27. Социально-психологические особенности студентов, склонных к виктимному поведению в интернет-пространстве / А.Р. Дроздикова-Зарипова, Н.Н. Калацкая, Р.А. Валеева [и др.]. — DOI 10.17513/snt.37852 // Современные наукоемкие технологии. — 2019. — № 12, ч. 1. — С. 159–166.

28. Anderson K.B. Off the Hook: Reducing Participation in Telemarketing Fraud / K.B. Anderson. — Washington, 2003. — URL: https://assets.aarp.org/rgcenter/consume/d17812_fraud.pdf.

29. Bricker D. Future of the world / D. Bricker. — URL: https://www.ipsos.com/sites/default/files/ct/news/documents/2019-11/a-more-dangerous-world-fear-2019.pdf.

30. Букин М. Лжевирусы атакуют / М. Букин // It Week. — URL: https://www.itweek.ru/security/article/detail.php?ID=126346.

31. Лунин А. Юристы-аферисты. Как разводят на деньги «борцы» с мошенниками / А. Лунин // Аргументы и факты. — 2020. — 22 сент. — URL: https://clck.ru/sXnLD.

32. Сахмеев В. В Москве накрыли колл-центр, сотрудники которого разводили «обманутых вкладчиков» / В. Сахмеев // Собеседник. — 2022. — 14 июня. — URL: https://sobesednik.com/private-finance/20220614-v-moskve-nakryli-koll-centr-sotrudniki.

33. Грустный Л. Бесплатный сыр: топ-6 разводов в Интернете / Л. Грустный // Kaspersky Daily. — URL: https://www.kaspersky.ru/blog/top-scam-schemes-2021/31551.

REFERENCES

1. Varchuk T.V., Vishnevskii K.V. *Victimology*. Moscow, Uniti-Dana Publ., 2008. 191 p.

2. Dagel P.S. «The Victim's Guilt» in Criminal Law. *Sovetskaya yustitsiya = Soviet Justice,* 1967, no. 6, pp. 10–11. (In Russian).

3. Kabanov P.A. Criminological Classification of Victims of Political Crimes in Modern Russian Criminal Political Victimology. *Yuridicheskoe obrazovanie i nauka = Juridical Education and Science,* 2007, no. 4, pp. 24–27. (In Russian). EDN: KFQFTJ.

4. Kim E.P., Mikhailichenko A.A. *Victimology: Problems of Theory and Practice.* Khabarovsk, 2004. 52 p. (In Russian).

5. Rivman D.V. *Criminal Victimology*. Saint Petersburg, Piter Publ., 2002. 304 p.

6. Tulyakov V.A. *Victimology*. *Social and criminological problems*. Odessa, Yuridichna Literatura Publ., 2000. 336 p. (In Russian).

7. Elkind P.S., Vandyshev V.V. Frank L.V. Victims of Crimes and Problems of Soviet Victimology. Dushanbe, «Irfon», 1977, 237 p. *Izvestiya vysshikh uchebnykh zavedenii. Pravovedenie = Proceedings of Higher Education Institutions. Pravovedenie,* 1978, no. 4, pp. 117–118. (In Russian). EDN: UCCMMV.

8. Stavitskii A. Windows were Attacked Through Icons. *Lenta.ru*. Available at: https://lenta.ru/news/2022/04/27/link. (In Russian).

9. Lomakin B., Gorin F. Fraudsters Gain Access to the Road Police Database. They Can Steal Cars and Send Fake Penalty Notices. *360tv.ru.* Available at: https://360tv.ru/news/tekst/dostup-k-baze-gibdd. (In Russian).

10. Yasakova E. SDEK Potentially Leaked Online the Database of its 25 mln Clients. *RBC*. Available at: https://www.rbc.ru/technology_and_media/15/07/2022/62d022d09a794711851de88dd. (In Russian).

11. Stimolo S. Coinbase Reveals Phishing Attack, 6000 Users Robbed. *The Criptonomist*. Available at: https://en.cryptonomist.ch/2021/10/05/coinbase-phishing-attack-6000-users-robbed.

12. Levkovich A. Hackers Attacked a Neurosurgery Center While a Child Was Being Operated on. *Vademecum*. Available at: https://clck.ru/sXmxG. (In Russian).

13. Kupriyanov S. «Russian Hackers» Were Spying on Hotel Guests Using the US NSA's Exploit. *Tekhnologii budushchego = Technologies of the Future*. Available at: http://alterprogs.ru/russkie-khakery-shpionili-za-postoyal.html. (In Russian).

14. Koteradze S. Cyberattacks «Reached Adulthood». Hackers Started to Cause Power Outages in Cities. *Eadaili*. Available at: https://eadaily.com/ru/news/2016/02/02/kiberataki-povzrosleli-hakery-nachali-otklyuchat-svet-v-gorodah. (In Russian).

15. Sidorenko E.L. *Victimological Provocation in Russian Criminal Law.* Stavropol State University Publ., 2005. 126 p.

16. Artem'ev N.S. Criminological Research of the Behavior of Violent Domestic Crime Victims. *Chelovek: prestuplenie i nakazanie = Human: Crime and Punishment,* 2018, vol. 26, no. 1, pp. 22–28. (In Russian). EDN: YUJQWJ.

17. Baturin A. Online Aggression: Counteraction Measures. *RedKrab*. Available at: https://redkrab.ru/blog/marketing/agressiya-v-internete-metodi-protivostoyaniya. (In Russian).

18. O'Moore M., Kirkham C. Self-esteem and its Relationship to Bullying Behavior. *Aggressive Behavior*, 2001, no. 27, pp. 269–283.

19. Swearer S.M., Song S.Y., Cary P.T., Eagle J.W., Mickelson W.T. Psychosocial Correlates in Bullying and Victimization: The Relationship Between Depression, Anxiety, and Bully/Victim Status. *Journal of Emotional Abuse*, 2001, no. 2, pp. 95–121. DOI: 10.1300/J135v02n02_07.

20. Georgiou S.N., Stavrinides P. Victims and Bully — Victims. Psychosocial Profiles and Attribution Styles. *School Psychology International*, 2008, vol. 29, iss. 5, pp. 574–589.

21. Cuadrado-Gordillo I., Antelo I. Cyberspace as a Generator of Changes in the Aggressive-Victim Role. *Computers in Human Behavior*, 2014, no. 36, pp. 225–233. DOI: 10.1016/j.chb.2014.03.070.

22. Nefedova M. Malware Developer Racoon Infected its Own System and Leaked its Data. *Khaker = Hacker*, 2021, no. 8. Available at: https://xakep.ru/2021/08/17/raccoon-leak. (In Russian).

23. Ivanov O. ART-group Patchwork Infected its Computers and Revealed Details of its Operations. *Anti-Malware*. Available at: https://clck.ru/u4WQ3. (In Russian).

24. Artem'ev N.S., Polishchuk E.G. Issues of the Victim Typology in Cases of Domestic Violence. *Vestnik Ryazanskogo gosudarstvennogo universiteta im. S.A. Esenina = Bulletin of Ryazan State University Named for S.A. Yessenin,* 2007, no. 17, pp. 82–90. (In Russian). EDN: NXMCRH.

25. Nikonov N. The site of the Public Chamber of Russia and the project «Feikam.net» were victims of a DDoS-attack. *Life*. Available at: https://life.ru/p/1332092. (In Russian).

26. Gurskaya N. The Site of Khimky Forest Defenders was Attacked by Hackers. *The Epoch Times*. Available at: https://www.epochtimes.ru/content/view/80124/3. (In Russian).

27. Drozdikova-Zaripova A.R., Kalatskaya N.N., Valeeva R.A., Kostyunina N.Yu., Biktagirova, G.F. Social-Psychological Features of Students Demonstrating Victim Behavior Online. *Sovremennye naukoemkie tekhnologii = Modern high technologies,* 2019, no. 12, pt. 1, pp. 159–166. (In Russian). DOI: 10.17513/snt.37852.

28. Anderson K.B. *Off the Hook: Reducing Participation in Telemarketing Fraud*. Washington, 2003. Available at: https://assets.aarp.org/rgcenter/consume/d17812_fraud.pdf.

29. Bricker D. *Future of the World*. Available at: https://www.ipsos.com/sites/default/files/ct/news/documents/2019-11/a-more-dangerous-world-fear-2019.pdf.

30. Bukin M. Fake Viruses Attack. *It Week*. Available at: https://www.itweek.ru/security/article/detail.php?ID=126346. (In Russian).

31. Lunin A. Lawyers-Swindlers. How «Anti»-Fraudsters Con People out of their Money. *Argumenty i Fakty*, 2020, September 22. Available at: https://clck.ru/sXnLD. (In Russian).

32. Sakhmeev V. Moscow Police Uncovered a Call Center Whose Employees Scammed «Deceived Bank Clients». *Sobesednik*, 2022, June 14. Available at: https://sobesednik.com/private-finance/20220614-v-moskve-nakryli-koll-centr-sotrudniki. (In Russian).

33. Grustnyi L. Free Cheese: Top Six Online Scams. *Kaspersky Daily*. Available at: https://www.kaspersky.ru/blog/top-scam-schemes-2021/31551. (In Russian).

ISSN 2500-4255

ИНФОРМАЦИЯ ОБ АВТОРЕ

Жмуров Дмитрий Витальевич — доцент кафедры уголовного права, криминологии и уголовного процесса Юридического института Байкальского государственного университета, координатор проекта «Национальная энциклопедическая служба России», кандидат юридических наук, доцент, г. Иркутск, Российская Федерация; e-mail: zdevraz@ya.ru.

ДЛЯ ЦИТИРОВАНИЯ

Жмуров Д.В. Кибержертва: особенности классификации / Д.В. Жмуров. — DOI 10.17150/2500-4255.2022.16(4).463-472. — EDN QFQHWL // Всероссийский криминологический журнал. — 2022. — Т. 16, № 4. — С. 463–472.

INFORMATION ABOUT THE AUTHOR

Zhmurov, Dmitry V. — Ass. Professor, Chair of Criminal Law, Criminology and Criminal Process, Law Institute, Baikal State University, Coordinator, Project «National Encyclopedic Service of Russia», Ph.D. in Law, Ass. Professor, Irkutsk, the Russian Federation; e-mail: zdevraz@ya.ru.

FOR CITATION

Zhmurov D.V. A Cybervictim: Specifics of Classification. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2022, vol. 16, no. 4, pp. 463–472. (In Russian). EDN: QFQHWL. DOI: 10.17150/2500-4255.2022.16(4).463-472.