УДК 343.988 **Д.В. Жмуров**

ПОНЯТИЕ КИБЕРВИКТИМНОСТИ

Аннотация

Статья посвящена одному из наиболее дискуссионных терминов современной виктимологии — кибервиктимности. Автором предложено его определение и рассмотрены основные типы (реактологический, социальный, технико-программный, ролевой). Кроме того, указываются основные критерии кибервиктимности как принципы и стандарты, на базе которых производится ее оценивание.

Ключевые слова: кибервиктимность, кибервиктимизация, кибервиктимология.

Если классическое понятие виктимности следует трактовать как отклонение от норм и правил безопасного поведения, то кибервиктимность — это несоответствие канонам и правилам безрисковой деятельности в информационной среде.

Значительное число ученых рассматривают виктимность как психическое или социально-психологическое отклонение, укоренившееся в ментальной природе индивида. Однако опыт исследования кибервиктимности позволяет добавить к этим компонентам еще и технический пункт. Действительно, повышенная склонность к тому, чтобы стать жертвой преступления, может детерминироваться не только особенностями личности, но и техническими (программными) недостатками функционала, который она использует для виртуализации и перехода в киберпространство. Например, когда терпит ущерб вследствие уязвимостей и критических ошибок в программном компоненте или на уровне поставщика услуг.

Для диагностики кибервиктимности могут использоваться различные методики, среди которых инцидентные опросники («Cyberbullying and Online Aggression Survey» S. Hinduja, J.W. Patchin в адаптации А.С. Голубовской), личностные опросники (русскоязычная версия опросника Big Five Inventory — BFI [1]) или специально разработанные виктимологические тест-анкеты (шкала кибервиктимности Д.В. Жмурова).

Кибервиктимность понимается прежде всего как нереализованная предрасположенность человека стать жертвой негативных обстоятельств в виртуальной среде. В связи с этим нельзя согласиться с мнением отдельных ученых о том, что виктимность — это деструктивное поведение целью которого становится намерение (осознанное или неосознанное) стать жертвой [2]. Если речь идет о намерении, то возможно, более точно говорить о саморазрушительном, аутодеструктивном поведении. При этом следует понимать, что многие из тех, кто обладает виктимными качествами, напротив, не хотят становиться жертвами.

Целесообразно выделить следующие типы кибервиктимности:

1. Реактологический, т.е. вызванный каким-либо аттитюдам (внутренним установкам), особенностям мышления, свойствам индивида, что предопределяют риск формирования статуса жертвы. Это могут быть как нормативные психические атрибуции (доверчивость, эгоцентризм, эксцентричность, нерешительность и т.п.), так и патологические качества потерпевших. Среди них особо выделяются психопатические признаки (патологическая трусость, истероидность, экзальтированность, ригидность и др.) или даже серьезные душевные нарушения (мазохизм, садизм, эксгибиционизм, патологический эротизм-нимфомания) [3].

2. Социальный предопределяет ведущую роль в генезе состояния потерпевшего таких характеристик, как пол, возраст, место жительства, отношение к религии, уровень образования и семейный статус. Довольно важными переменными, по которым предстоит анализ их виктимогенного вклада, являются статус домохозяйств, интересы, ценности, включенность в различные социальные группы. Таким образом, изучение социально-демографических характеристик потерпевших по праву является отправной точкой проведения виктимологических изысканий [4].

3. Технико-программный составляет случаи существенного вклада технологического компонента в завершенную картину виктимизации. «Жертвенность» индивида определяется некоторыми объективными моментами, в частности, а) отставанием систем безопасности от уровня развития хакерских технологий,

когда меры защиты начинают разрабатываться уже после совершенных атак; б) низким уровнем безопасности многих программ, что связано с желанием разработчика сэкономить, не проводить полноценное стресс-тестирование, как можно скорее выпустить продукт на рынок и пр.; в) повсеместным распространением вредоносных программ, которые используются как средство заработка, орудие недобросовестной конкуренции, инструмент борьбы за идеи или способ показать свою компетентность. В любом случае пользователь обречен на существование в цифровом мире, переполненном вирусами, червями, руткитами и бэкдорами.

4. Ролевой связан с характеристикой социальной роли человека независимо от его личностных свойств, повышающей опасность посягательства лишь в силу исполнения этой роли [5]. Некоторые ролевые предписания включают в себя виктимогенное содержание, например клиент банка, покупатель, любовник, инвестор, безработный, собственник и пр.

При этом нельзя не учитывать так называемую виктимогенную деформацию личности, понимаемую как сочетание личностных и поведенческих характеристик, связанных с неблагоприятными особенностями социализации [5]. Стимулируя правонарушающее поведение по отношению к своему носителю, она может содержать признаки нескольких указанных типов кибервиктимности.

Критериями кибервиктимности выступают принципы и стандарты, на базе которых производится оценка ее наличия или отсутствия, а также степени выраженности. Таковыми могут быть:

– склонность к провоцирующему поведению, т.е. таким формам действий, которые создают реальную возможность и способствуют реализации преступных намерений [6] (высокая частота нахождения в социальных сетях, большой объем общедоступной и скрытой информации о личности; использование сомнительных ресурсов и приложений);

– низкая частота использования защитных стратегий (использование устаревших и сопряженных с риском технологий; низкий уровень осведомленности об аспектах информационной безопасности, цифровая незащищённость членов семьи и т.п.);

– цифровая погруженность, как глубина вхождения личности в виртуальный мир. Результаты исследований некоторых

ученых показывают, что кибервиктимность тесно связана с компьютерной зависимостью [7];

– опыт предыдущей кибервиктимизации как один из индикаторов рискованного поведения в биографическом контексте.

Таким образом, кибервиктимность представляет собой самостоятельную и немаловажную проблему. Она явно выходит за привычные виктимологические рамки, предопределяя нетрадиционные подходы к оценке ее моделей, процессу реализации и субъектам. В первую очередь это обусловлено новыми качествами среды, в которых происходит виктимизация. Её отличают деперсонализация, депсихологизация, ранее не фиксируемые формы воплощения и не регистрируемые до этого масштабы. Виктимизация в интернет-среде вносит важные поправки в традиционные представления о реализации виктимного потенциала.

Список использованной литературы

1. Вихман А.А. Динамика личностных показателей в зависимости от опыта кибербуллинга в ранней юности // Международная научно-практическая конференция «Личность в норме и патологии», 22–23 апреля 2021 г.

2. Юдина А.М., Дементьев А.Г. Превенция виктимного поведения студенческой молодежи в сети Интернет // Современное педагогическое образование. 2021. № 7. С. 91–94.

3. Максименков А.А., Майоров А.В. Психологические аспекты виктимности // Виктимология. 2015. № 4 (6). С. 26–30.

4. Будкина И.С. Социально-демографическая характеристика личности несовершеннолетних жертв преступлений (региональное исследование) // Общество: политика, экономика, право. 2018. № 12 (65). С. 119–123.

5. Репецкая А.Л. Виновное поведение потерпевшего и проблемы реализации принципа справедливости в уголовной политике : автореф. дис. … канд. юрид наук. Москва : МГУ, 1992. 26 с.

6. Коновалова В.Е., Шепитько В.Ю. Основы юридической психологии. Харьков, 2005. С. 147–149.

7. Вихман А.А., Волкова Е.Н., Скитневская Л.В. Традиционные и цифровые возможности профилактики кибербуллинга // Вестник Мининского университета. 2021. Т. 9, №4. С. 10.

Информация об авторе

Жмуров Дмитрий Витальевич — кандидат юридических наук, доцент, доцент кафедры уголовного права и криминологии, Институт юстиции, Байкальский государственный университет, г. Иркутск.