УДК 343.988

ПОСЛЕДСТВИЯ КИБЕРВИКТИМИЗАЦИИ И ЕЕ ОСНОВНЫЕ ПРИЗНАКИ

Д.В. Жмуров
Байкальский государственный университет, г. Иркутск, Российская Федерация, zdevraz@ya.ru

Аннотация. В статье рассматривается проблема последствий кибервиктимизации. Предложено авторское определение данного понятия. Дается указание на материальные показатели последствий кибервиктимизации и вместе с тем ставится вопрос об актуальности ее комплексной оценки, включающей психический, организационный и иные виды ущерба. Выделяются позитивные и негативные итоги кибервиктимизации. Для негативных последствий (т.е. наступающего вреда) предложены основные признаки, среди которых: регрессивность, дуалистичность, иррадиированность, полиморфность, ситуационность, диспропорциональность.

Ключевые слова: кибервиктимизация, кибервиктимность, последствия кибервиктимизации, кибержертва.

THE CONSEQUENCES OF CYBERVICTIMISATION AND THEIR KEY ATTRIBUTES

D.V. Zhmurov
Baikal State University, Irkutsk, the Russian Federation, zdevraz@ya.ru

Abstract. The article deals with the problem of the consequences of cyber victimization. The author's definition of this concept is proposed. It points to material indicators of cyber victimization consequences and, at the same time, raises the question about the relevance of its comprehensive assessment, including mental, organizational and other types of damage. Positive and negative outcomes of cybervictimization are identified. For negative outcomes (i.e., the coming harm), the main features are proposed, including regressiveness, duality, irradiation, polymorphism, situationality, and disproportionality.

Keywords: cybervictimization, cybervictimization, cyber consequences, cyber victimization.

Как известно, в юридических науках под виктимизацией понимается процесс превращения лица в жертву правонарушения (преступления или деликта). Подобные инциденты наблюдается сегодня не только в привычном формате – в быту, на улицах и транспорте, но и в виртуальных средах, что само по себе не может оставаться без внимания научного сообщества. Этим объясняется интенсификация исследований в данной области и появление новых субдисциплин, таких как цифровая криминология, кибервиктимология и киберкриминалистика.

Актуальным теоретическим вопросом, среди прочих других, является тема оценки последствий кибервиктимизации, т.е. ее негативных результатов, возникающих для потерпевшего (имущественных, психологических, организационных и проч.). К сожалению, на данный момент имеются лишь приблизительные оценки состояния проблемы. По ориентировочным подсчетам специалистов, ущерб мировой экономике от киберпреступности будет ежегодно расти и к 2025 году достигнет 10,5 триллионов долларов [2]. Для того, чтобы понимать масштабы этих процессов достаточно упомянуть, что в 2013 году данный показатель не превышал 113 миллиардов долларов [1]. Несомненно, речь идет о финансовых преступлениях (интернет-мошенничество, цифровая кража), тогда как ущерб от случаев насильственной виктимизации (кибербуллинг, кибертерроризм, интернет-преследование) в расчет не берется.

Полагаем, что необходимо смысловое разделение терминов «вред от кибервиктимизации» и «последствия кибервиктимизации». Содержательное наполнение указанных понятий не совпадает. Если говорить о последствиях, то они могут характеризоваться как положительные, так и отрицательные. Вред, напротив, интерпретируется только в негативном плане, являясь одним из возможных, но не единственным итогом виктимизации в сети. Если с экономическим инструментарием расчета ущерба от кибервиктимизации есть хоть какая-то ясность, то формализация психологических, физиологических и моральных издержек является чрезвычайно сложной задачей. Как, например, в денежном эквиваленте оценить депрессивные или суицидальные эпизоды, возникающие у жертвы кибербуллинга? Или произвести учет ухудшения качества жизни у лиц, подвергшихся систематическому сексуальному киберпреследованию?

Таким образом, термин «последствия кибервиктимизации» целесообразно определить как результат противоправного воздействия на субъекта виртуальной коммуникации.

Это могут быть различные изменения: начиная со сферы индивидуальной психологии (модификация самоотношения, самосознания) и заканчивая

организационно-ориентированной (снижение качества управления в компании). В результате данную ситуацию можно описать как эустресс (оказывает положительное влияние на субъекта) или дистресс (демонстрирует негативное или разрушительное воздействие). Таким образом, можно с уверенностью предположить, что кибервиктимизация влечет как вредные, так и негативные последствия.

К первой группе относятся: совершенствование адаптивных навыков, воспитание привычки противодействия обидчикам, развитие рефлексивного отношения к собственной деятельности и, как следствие, умения планировать свои поступки, выработка поведенческой гибкости и навыков противостояния противнику в конфликтных ситуациях; получение бесценного негативного опыта, который в дальнейшем поможет преодолевать сложные жизненные ситуации.

Ко второй группе относятся: материальные и иные потери, снижение эффективности деятельности, падение качества дальнейшей жизни, появление негативных эмоциональных состояний и психологических проблем, косвенные издержки для общества и аффилированных лиц и т.п.

Обратим особое внимание на некоторые признаки второй группы последствий негативной модальности:

1. *Регрессивность* – это качественное изменение положения объекта в сторону ухудшения его жизненного (витального) уровня. Проявляется в многочисленных неблагоприятных результатах: утрате ценностей, лишении каких-либо возможностей, потерях, убытках, страданиях, внезапных дисфункциональных изменениях самочувствия и здоровья, приостановке экономической деятельности, утрате контроля над компонентами цифровой среды и проч.

2. *Дуалистичность*, как виртуально-реальная сущность наносимого вреда. С одной стороны, действия, которые выступают его причиной, имеют цифровую природу, проявляясь исключительно в киберпространстве, но с другой – нельзя не видеть материальность и осязаемость ущерба, выходящего за границы виртуальной жизни (потеря реальных ценностей, нарушение циклов производства и торговли, угроза здоровью и жизни). Другими словами, негативные последствия цифровой виктимизации продолжаются офлайн, в реальной жизни.

3. *Иррадиированность* предполагает, что негативные последствия претерпевает не только жертва, но и третьи лица, не обязательно связанные с ней. Последствия кибервиктимизации, как «круги на воде» расходящиеся экстенсивно – не в глубь, а вширь. И чем больше времени проходит, тем больший радиус колебаний можно увидеть. Если это сравнение уместно, то

негативные последствия киберпреступлений, как упомянутые «круги», не ограничиваются только жертвой, они почти всегда выходят за ее индивидуальные рамки и проявляются в иных социальных отношениях. Таким образом, вред, кроме самой жертвы, причиняется другим субъектам. Например, в случае DDoS-атаки на сайт, как правило, кроме его собственника страдают еще и поставщик DNS-услуг; добросовестные пользователи хостинга, где был размещен атакуемый ресурс; получатели услуг отключенных веб-проектов; иные субъекты цифровой экономики, связанные с пострадавшим, особенно, если последний был включен в цепь поставок и т.д.

4. *Полиморфность* – означает такое качество последствий, когда они сочетают в себе формализованные и неформализованные характеристики. То есть помимо экономических индикаторов вреда, объективизированных суммой ущерба или затратами на восстановление, существуют вредные последствия, не поддающиеся точному подсчету (ухудшение качества жизни, риски осуществления девиаций, соматические и психические опасности).

5. *Ситуационность,* когда ущерб зависим от множества не всегда просматриваемых обстоятельств. Например, оценка вреда при атаке на веб-сайт компании зависит не только от стоимости часа простоя ресурса и упущенной выгоды, но также и от затрат на устранение вредных последствий, устанавливаемых на локальных рынках по-разному. В США или Германии – это будет одна цена, в России – совсем другая. Аналогичная ситуация с психическими реакциями жертв. Они будут зависеть от особенностей национальной ментальности и специфики этнопсихологии, преобладающей в поведении жертвы. Признак ситуационности напрямую зависит от территориальных, антропологических, межкультурных, экономических и других факторов.

6. *Диспропорциональность* заключается в том, что между потраченными ресурсами на реализацию преступных намерений и причиняемым ущербом, как правило, обнаруживается серьезное несоответствие: нередко, в интернете малыми усилиями достигаются серьезные негативные результаты.

Итак, последствия кибервиктимизации – глобальная проблема современного мира. Они влияют на все сферы жизни человека, от экономики до интеллектуальной деятельности. В то же время они сильно различаются: от единичных случаев кибервиктимизации (интернет-угрозы, кибермошенничества) до массовых (кибертерроризм). Оценка ущерба от кибервиктимизации занимает особое место в изучении реального состояния киберпреступности, а также при разработке комплекса ее теоретико-методологических и профилактических мероприятий.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Пархоменко С.В. Предупреждение компьютерной преступности в Российской Федерации: интегративный и комплексный подходы / С.В. Пархоменко, К. Н. Евдокимов // Криминологический журнал Байкальского государственного университета экономики и права. – 2015. – Т. 9, № 2. – С. 265–276. – DOI: 10.17150/1996- 7756.2015.9(2).265-276.

2. Эксперт оценил ущерб от киберпреступлений в России в 2021 году. – URL: https://ria.ru/20211222/kiberprestupleniya-1764832102.html (дата обращения: 31.08.2022).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Жмуров Дмитрий Витальевич – кандидат юридических наук, доцент, Байкальский государственный университет, г. Иркутск, Российская Федерация, zdevraz@ya.ru.

INFORMATION ABOUT THE AUTHOR

Dmitry V. Zhmurov – PhD in Law, Associate Professor, Baikal State University, Irkutsk, Russian Federation, zdevraz@ya.ru.