КИБЕРВИКТИМОЛОГИЯ: ПОНЯТИЕ И СОСТАВЛЯЮЩИЕ ЭЛЕМЕНТЫ

Исраелян Геворг Вовaевич
Начальник Научно-исследовательского центра прикладных проблем криминологии Национального бюро экспертиз Национальной академии наук Республики Армения, преподаватель Международного университета Евразия, кандидат юридических наук, доцент

Криминальная виктимология традиционно изучает жертву преступления, предрасположенность человека к тому, чтобы стать жертвой преступления - виктимность, процесс становления жертвы преступления - виктимизацию, на основании чего создаются меры виктимологического предупреждения преступлений. В течение долгого времени основные концепции криминальной виктимологии, как правило, основывались на непосредственной, часто физической связи между преступником и потерпевшим. Однако в современных условиях широкого пользования населением цифровыми технологиями отмечаются существенные изменения в укладе взаимодействия сторон криминального акта. Также наблюдается рост числа киберпреступлений. Данные обстоятельства обусловили создание нового направления криминальной виктимологии – кибервиктимологии.

Автор определяет понятие «кибервиктимология». Так, кибервиктимология - это направление криминальной виктимологии, которая изучает кибержертву, кибервиктимность, кибервиктимизацию.

В качестве структурных элементов кибервиктимологии автор выделяет кибержертву, кибервиктимность, кибервиктимизацию.

Ключевые слова: кибервиктимология, кибержертва, кибервиктимность, кибервиктимизация, киберпреступление.

Введение

Криминальная виктимология традиционно изучает жертву преступления и связанные с ней понятия - виктимность, т.е. предрасположенность человека стать жертвой преступления, виктимизацию, т.е. процесс становления жертвы

преступления, на основании чего создаются меры виктимологического предупреждения преступлений [1].

В течение долгого времени основные концепции криминальной виктимологии, как правило, основывались на непосредственной, часто физической связи между преступником и потерпевшим, например, лишение жизни потерпевшего, нанесение вреда здоровью потерпевшего и т.п. Однако в современных условиях, когда все сферы общественной жизни насыщены кибертехнологиями, рост киберпреступности очевиден, естественно, появилась необходимость формирования нового направления криминальной виктимологии относительно к киберпреступности - кибервиктимологии.

Следует отметить, что в зарубежных странах имеется теоретический и практический опыт по обсуждаемой проблеме. Например, в 2021 г. в США вышла в свет книга автора Дебарати Халдер (Debarati Halder) «Кибервиктимология» (Cyber Victimology). Есть достижения также в практическом плане. Так, на протяжении вот уже нескольких лет в США октябрь объявляется месяцем осведомленности о кибербезопасности, что стало хорошей традицией. Не стал исключением и октябрь 2022 г. Во главе с Федеральным бюро расследований США партнерские агентства призывают граждан защищать свои цифровые устройства и информацию, хранящуюся онлайн, от преступников, давая при этом соответствующие рекомендации по соблюдению «кибергигиены», и не забывать сообщать о случаях компрометации данных или попытках завладеть ими через специальную форму на сайте Центра жалоб на интернет-преступления. ФБР осуществляет так же меры индивидуального кибервиктимологического характера [2, с. 54, 58].

В Российской Федерации так же развивается кибервиктимология, о чем свидетельствуют результаты исследований таких авторов, как Д.В. Жмуров, С.А. Стяжкина и др. [3].

В Республике Армения обсуждаемая проблема не изучена. Данный факт обусловливает актуальность и новизну исследования, изложенную в настоящей статье.

Целью исследования является раскрытие содержания понятия «кибервиктимология» и описание характерных особенностей его составляющих частей.

Основное исследование

В последнее время все чаще упоминается новое понятие - «кибервиктимология». Предпосылками для формирования данного направления криминальной виктимологии, на наш взгляд, являются следующие факторы:

1. Учёные-виктимологи приписывают контакту преступника и жертвы некоторую психологическую согласованность. Считается, что жертва выбирается «не случайно, а по точным критериям и характеристикам». Преступник и пострадавший психологически подходят друг другу, по выражению одного из основателей виктимологии Ганса фон Гентига (1888–1974), как «замок и ключ». Киберпреступность своим существованием, напротив, ставит под сомнение данное положение. Во многом она основана на случайном, рандомизированном выборе жертв. Кроме того, отмечаются существенные изменения в укладе взаимодействия сторон криминального акта. Одной из важных идей криминального воздействия в киберпространстве становится отказ от прямого воздействия на потерпевшего, стремление максимально замаскировать свои действия, если это возможно. Часто жертвы даже не подозревают, что им причиняется урон. Это пример избегания открытой конфронтации и явной агрессии со стороны преступников новой формации. Подобная стратегия гарантирует им безопасность, как правило, исключает мотивацию возмездия у пострадавшей стороны. Например, при криптоджекинге, когда компьютер или смартфон жертвы используются без её разрешения, причем не для кражи данных, а для того, чтобы киберпреступники могли «добывать» криптовалюты без использования своих собственных ресурсов [4, с. 115-118].

2. В классической виктимологии важное значение имеет действие виктимогенных личностных и виктимогенных ситуационных факторов. Первое - это уязвимость индивида, второе - условия внешней среды, детерминирующие поведение потерпевшего. В обоих случаях жертва активна, именно она стимулирует преступное поведение своими уязвимостями, либо ситуационной деятельностью. В киберпреступности детерминационные связи между преступником и жертвой усложняются и не исчерпываются причинностью или условиями взаимодействия этих сторон. Например, личностные и ситуационные факторы виктимности не будут иметь значения при совершении акта кибертерроризма, когда дестабилизируется система энергоснабжения. Эти действия, в свою очередь, могут привести к локдауну на критически важных узлах (транс-

порте, здравоохранении и проч.). А пострадавшие при этом люди (например, больные на операционном столе, пассажиры автоматических транспортных средств) абсолютно не будут демонстрировать ни личностных, ни ситуационных факторов виктимности [5, с. 115-118].

3. Отмечаются совершенно нетипические случаи возникновения виктимных сообществ, представляющих массовые объединения потенциальных жертв, каждая из которых надеется таковой не стать («эпименические ульи» или «консорциумы жертв»). Например, так происходит в хайп-проектах, которые фактически представляют собой финансовые пирамиды с тысячами участников. Каждый из них надеется заработать и не опоздать вывести средства до того, как всё окончательно рухнет. Часто организаторы этих пирамид даже не скрывают истинных целей проекта, а инвесторы - «потенциальные жертвы» понимают, что их доходы складываются из взносов вновь прибывших участников. Поэтому им ничего не остается, кроме того, как привлекать новичков. Получается так, что жертвы сами ищут новых жертв. Как только поток неофитов иссякнет, они станут фактическими потерпевшими, рассчитывая, конечно, что до этого не дойдет. Таких «союзов жертв», где каждый надеется не оказаться последним, в интернете предостаточно [5, с. 115-118].

Основываясь на вышеуказанном, кибервиктимологию можно определить как направление криминальной виктимологии, которая изучает кибержертву, кибервиктимность, кибервиктимизацию.

Исходя из указанного элементами предмета изучения кибервиктимологии являются:

1. Жертва киберпреступления - кибержертва.

В юридической литературе кибержертва определяется как организация, группа или человек, пострадавший от уголовно-наказуемых актов, реализованных преимущественно в цифровой среде [3, с.547]. С нашей точки зрения, в определении «кибержертва» должна быть указана не только сфера - цифровая среда, но и способ и средства совершения преступлений, а также использование цифровых технологий. Таким образом считаем, что кибержертва - это человек, группа лиц, организация, которые пользуются цифровыми техническими средствами и по отношении к которым совершено преступление с использованием цифровых технологий.

2. Кибервиктимность.

Кибервиктимность - это предрасположенность стать жертвой киберпреступления. Исходя из вышепредложенного понятия «кибержертва» можно выделить виды кибервиктимности:

1) Индивидуальная кибервиктимность.

Индивидуальная кибервиктимность - свойство индивидуума, обусловленное, как правило, психологическими качествами, при использовании цифровых технологий стать кибержертвой. Например, доверчивость, неосмотрительность жертвы, по отношению к которой совершается кибермошенничество.

2) Групповая кибервиктимность.

Групповая кибервиктимность проявляется относительной предрасположенностью стать жертвой киберпреступлений таких групп лиц, которым характерны общие объединяющие признаки, например, сообщество IT-специалистов.

3) Массовая кибервиктимность.

Массовая кибервиктимность - это предрасположенность стать жертвой киберпреступлений при определенных условиях, например, при целевых кибератаках на те цифровые средства, которые никак не защищены.

3. Кибервиктимизация.

Кибервиктимизация - процесс становления жертвы киберпреступления. Она непосредственно связана с преступными кибердействиями и является их результатом. На индивидуальном уровне кибервиктимизация содержит следующие элементы:

1) Объект кибервиктимизации.

Объектом кибервиктимизации являются общественные отношения, охраняемые уголовным законом, которым причинается вред или создается для этого угроза в связи с кибердействиями.

2) Объективная сторона кибервиктимизации.

Объективная сторона кибервиктимизации - это ситуация, в котором реализуется кибервиктимизация и которая влючает место, время, способ совершения киберпреступления и т.д.

3) Субъект кибервиктимизации.

Субъектом кибервиктимизации является кибержертва.

4) Субъективная сторона кибервиктимизации.

Субъективная сторона кибервиктимизации включает состояние субъекта, факторы, влияющие на его поведение и т.д. [4, с. 80-83].

Конечно, кибервиктимность и кибервиктимизация - явления непосредственно связанные с кибержертвой, однако для углубленного изучения предлагаем их рассматривать в качестве самостоятельных элементов кибервиктимологии.

Заключение

В современных условиях широкого пользования населением цифровыми технологиями, естественно, возрасло число киберпреступлений. Данный факт, а также специфика механизма киберпреступлений обусловили создание нового направления криминальной виктимологии - кибервиктимологии.

Кибервиктимологию можно определить как направление криминальной виктимологии, которая изучает кибержертву, кибервиктимность, кибервиктимизацию. Элементами предмета изучения кибервиктимологии являются: кибержертва, кибервиктимность, кибервиктимизация.

Список литература

1. Малкина-Пых И. Виктимология. Психология поведения жертвы //https://www.libfox.ru/420727-2-irina-malkina-pyh-viktimologiya-psihologiya-povedeniya-zhertvy.html#book (дата доступа: 17.05.2023).
2. Пейзак А.В. Противодействие киберпреступности в США //Общество, право, государственность: ретроспектива и перспектива, 2022, № 4 (12). С. 54-59.
3. Стяжкина С.А. Виктимологическая профилактика кибермошенничества //Вестник Удмуртского университета. Экономика и право, 2022. Т. 32, вып. 3, с. 546-552.
4. Жмуров Д.В. Кибервиктимность как новая категория виктимологии постмодерна //Азиатско-тихоокеанский регион: экономика, политика, право, 2021, № 2., с. 113-122.
5. Ривман Д.В. Криминальная виктимология. СПб.: Питер, 2002. – 304 С:

CYBER VICTIMOLOGY: CONCEPT AND CONSTITUENT ELEMENTS

Gevorg Israyelyan
Head of the Scientific Research Center
of Applied problems in criminology of
National Bureau of Expertise of
National Academy of Sciences of the Republic of Armenia,
Lecturer at Eurasia International University,
Candidate of Legal sciences, Associate Professor

Criminal victimology traditionally examines the victim of crime, the predisposition of a person to become a victim of crime - victimization, the process of becoming a victim of crime – victimization, on the basis of which measures of victimological crime prevention are created. For a long time, the basic concepts of criminal victimology, as a rule, were based on the direct, often physical connection between the offender and the victim. However, in modern conditions of widespread use of digital technologies by the population, there are significant changes in the way of interaction between the parties to a criminal act. There is also an increase in the number of cybercrimes. These circumstances led to the creation of a new direction of criminal victimology – cyber victimology.

The author defines the concept of cyber victimology. So, cyber victimology is a branch of criminal victimology that studies cyber-sacrifice, cyber-victimization, cyber-victimization.

As structural elements of cyber victimology, the author identifies cyber-sacrifice, cyber-victimization, cyber-victimization.

Key words: cyber victimology, cyber-victimation, cyber-victimization, prevention.

Հոդվածը գրախոսվել է՝ 19. 05.2023թ.:
Ներկայացվել է տպագրության՝ 01.06.2023թ.: