Дата поступления рукописи в редакцию: 06.05.2025 г.
Дата принятия рукописи в печать: 16.06.2025 г.
DOI: 10.24412/2782-3830-2025-5-261-263

ЖМУРОВ Дмитрий Витальевич,
к.ю.н., доцент кафедры
уголовного права и криминологии
Байкальского государственного университета
(г. Иркутск),
e-mail: zdevraz@ya.ru

ДОКТРИНАЛЬНЫЕ ПОХОДЫ К ПРЕДМЕТУ КИБЕРВИКТИМОЛОГИИ

Аннотация. *В статье выделяются и подробно раскрываются четыре ключевых исследовательских подхода к предмету кибервиктимологии: антропологический (акцент на когнитивных, эмоциональных и поведенческих особенностях кибержертв), юридический (догматический, оперирующий категориями правосубъектности), криминологический (рассматривающий последствия киберпреступности для групп, общества и государства на макроуровне) и технический (анализирующий уязвимости информационно-коммуникационных систем). Автор подчеркивает невозможность изолированного применения отдельных подходов в современном цифровом ландшафте, где комплексная виктимизация становится всё более типичной.*

Ключевые слова: *кибервиктимология, кибержертва, кибервиктимизация, киберпреступность, цифровая безопасность.*

ZHMUROV Dmitry Vitalievich,
PhD in Law, Associate Professor,
Department of Criminal Law and Criminology,
Baikal State University
(Irkutsk)

DOCTRINAL APPROACHES TO THE SUBJECT OF CYBERVICTIMOLOGY

Annotation. *The article identifies and elaborates on four key research approaches to the subject of cyber victimology: anthropological (focusing on the cognitive, emotional and behavioural characteristics of cyber victims), legal (dogmatic, operating with categories of legal personality), criminological (examining the consequences of cybercrime for groups, society and the state at the macro level) and technical (analysing the vulnerabilities of information and communication systems). The author stresses the impossibility of isolated application of individual approaches in the modern digital landscape, where complex victimisation is becoming more and more typical.*

Key words: *cybervictimology, cybervictimization, cybervictimization, cybercrime, digital security.*

Кибервиктимология - это сфера научных интересов, направленная на выработку системно организованных, непредвзятых и обоснованных знаний о «цифровой действительности» и виктимном поведении человека в ней. Одной из главных задач последней выступает изучение виктимизации пользователей ИТТ. Кибервиктимология исходит из понимания того, что киберпреступления могут наносить серьезный ущерб не только материальному, но и физическому, психологическому, эмоциональному благополучию индивида [1].

В предмет кибервиктимологии входят следующие элементы:

- криминальная кибервиктимизация (структура, оценка последствий, паттерны протекания, особенности детерминации);
- кибержертва и её типы (систематизация кибержертв);
- криминальная кибервиктимность, как фактор, обусловливающий кибервиктимизацию;
- детерминанты криминальной кибервиктимизации;
- система виктимологического воздействия на киберпреступность: виктимологическая профилактика кибервиктимности;

– стратегии минимизации и компенсации нанесенного вреда для случаев реализованной виктимности.

В современной кибервиктимологии кристаллизуется целый спектр исследовательских «ракурсов», через которые ученые рассматривают представленные выше элементы, в частности, фигуру кибержертвы и феномены виктимизации (виктимности) в цифровой среде.

В итоге складывается многослойная модель, где каждый слой - результат особого дисциплинарного фокуса, собственных категорий и методик. Базовыми, по-видимому, остаются четыре подхода - антропологический, юридический, криминологический и технический. На практике они редко существуют изолированно, однако для аналитической ясности их целесообразно развернуть по отдельности и подчеркнуть, какие вопросы каждый из них поднимает и какие ограничения таит в себе.

Антропологический подход строится вокруг допущения, что основной носитель виктимогенных характеристик - физическое лицо как биосоциальное существо. Первостепенное внимание здесь уделено когнитивным, эмоциональным и поведенческим предпосылкам того, почему индивид оказывается восприимчив к манипуляциям, социальной инженерии, технически простым, но психологически изощренным способам дискредитации. Особое место в исследовании кибервиктимизации занимают такие параметры, как цифровая грамотность, устойчивость к стрессу, социальный статус, поведенческие особенности, личностные качества, биологические характеристики, например, половая принадлежность [2]. Антропологический ракурс, таким образом, фокусируется на «внутренней» стороне виктимности и показывает, как именно информационно-психологический контекст трансформируется в сетевые уязвимости. Этот подход является базовым, поскольку многие киберпреступления направлены на причинение вреда именно людям, даже если непосредственной атаке подвергаются технические системы или организации.

Догматический (юридический) подход трактует кибержертв, опираясь на нормативные конструкции: субъект преступления, объект посягательства, правосубъектность и проч. Линия разграничения здесь не проводится по биологическому признаку: кибержертвой признается всякий носитель прав и законных интересов, чьи охраняемые права ущемляются. Отсюда логично включение в круг кибержертв юридических лиц, индивидуальных предпринимателей, публично-правовых образований и даже наднациональных структур, если они наделены правосубъектностью по международному или внутригосударственному праву. В данном случае важен не столько индивидуальный опыт виктимизации (моральный или физический ущерб), сколько факт нарушения прав и законных интересов организаций (экономические и репутационные потери, разглашение коммерческой тайны, срыв производственных процессов и т.п.).

Криминологический подход расширяет границы еще радикальней: кибержертвами он предлагает считать не только физических и юридических лиц, но и социальные общности (например, этнические или социальные группы, подвергающиеся целенаправленным информационным атакам или разжиганию ненависти онлайн), а также государство и его структурные элементы (органы власти, критическая инфраструктура, национальная безопасность). Следовательно, потенциал кибервиктимизации выходит далеко за рамки индивидуального уровня и затрагивает коллективных, публичных, культурных и даже символических реципиентов ущерба. Киберпреступность вполне способна оказывать негативное влияние на политическую стабильность, дискредитировать государственные институты, подрывать доверие к демократическим процедурам. Следовательно, объектом виктимизации могут быть не только частные лица и корпорации, но и само государство, его инфраструктура, национальные и конфессиональные общности [3]. В этом смысле кибервиктимология криминологического толка приближается к социологии риска, рассматривая киберугрозы как фактор макросоциальной неустойчивости. Криминологический подход позволяет анализировать киберпреступность как угрозу не только частным интересам, но и обществу (государству) в целом, разрабатывая стратегии противодействия на глобальном уровне.

Технический подход вводит в терминологический оборот феномен иного актора цифрового пространства. С такой точки зрения, непосредственным объектом атаки и, следовательно, «жертвой» в определенном смысле, выступают технико-технологические субъекты. К ним относятся компьютеры, серверы, мобильные устройства, коммуникационные сети (локальные, глобальные), программное обеспечение, информационные платформы, базы данных и т.д. Здесь центр тяжести перемещается на уязвимости аппаратного и программного характера, модели искусственного интеллекта, «умные» устройства и т.п. Техника обретает почти юридическую субъективацию: она «страдает», «портится», «становится недоступной». Технический подход акцентирует внимание на том, что именно информационно-технологическая система зачастую становится точкой входа преступника, а значит, виктимологический анализ нельзя сводить только к изучению человеческих ошибок.

Необходимо подчеркнуть, что в реальности эти исследовательские подходы пересекаются и взаимообусловлены. По мере усложнения цифрового ландшафта все чаще возникают ситуации комплексной виктимизации. Например, вредоносное вмешательство в автоматизированную систему управления очистными сооружениями может одновременно порождать: во-первых, имущественный и экологический ущерб для хозяйствующего субъекта (догматический подход); во-вторых, загрязнение акватории и гибель биологических видов (криминологический подход); в-третьих, угрозу здоровью населения прибрежных территорий (антропологический подход). В такой конфигурации становится очевидной ограниченность монофокусного анализа и востребованность синтеза отраслевых методологий.

Развивая эту мысль далее, можно указать на несколько новых осей, которые постепенно встраиваются в существующий набор подходов. Во-первых, эколого-биологическая перспектива, трактующая природные объекты как адресаты киберрисков, особенно на фоне внедрения интернета вещей в сельском хозяйстве и климатическом мониторинге. Во-вторых, культурно-медиационный вектор, где «жертвой» признается коллективная идентичность или символический капитал группы, чьи ценности подверглись подмене или разрушению через информационное воздействие. В-третьих, экономико-системный ракурс, описывающий разрушение цепочек поставок, логистических узлов и финансовых экосистем в терминах «кибервиктимности рынков». В-четвертых, усложняющаяся технологическая траектория, связанная с признанием субъектности искусственного интеллекта и необходимостью принятия его в качестве кибержертвы.

Итоговое теоретическое поле киберкриминологии напоминает многомерную карту, на которой каждая точка может быть одновременно людской, юридической, догматической или технической. Задача современной науки - не пристегнуть очередную категорию к существующему списку, а разработать методологию, способную моделировать взаимодействие разных типов жертв, оценивать каскадные эффекты и предлагать системы превентивных мер, соответствующие этой многоуровневой реальности.

Список литературы:

[1] Коробеев А.И., Дремлюга Р.И., Кучина Я.О. Киберпреступность в Российской Федерации: криминологический и уголовно-правовой анализ ситуации // Всероссийский криминологический журнал. 2019. № 3 (13). С. 416–425

[2] Бочкарева Е.В., Стренин Д.А. Теоретико-правовые аспекты кибербуллинга // Всероссийский криминологический журнал. 2021. № 1 (15). С. 91–97

[3] Дремлюга Р.И., Коробеев А.И., Федоров А.В. Кибертерроризм в Китае: уголовно-правовые и криминологические аспекты // Всероссийский криминологический журнал. 2017. № 3 (11). С. 607–614

Spisok literatury:

[1] Korobeev A.I., Dremlyuga R.I., Kuchina Ya.O. Kiberprestupnost' v Rossijskoj Federacii: kriminologicheskij i ugolovno-pravovoj analiz situacii // Vserossijskij kriminologicheskij zhurnal. 2019. № 3 (13). S. 416–425

[2] Bochkareva E.V., Strenin D.A. Teoretiko-pravovye aspekty kiberbullinga // Vserossijskij kriminologicheskij zhurnal. 2021. № 1 (15). S. 91–97

[3] Dremlyuga R.I., Korobeev A.I., Fedorov A.V. Kiberterrorizm v Kitae: ugolovno-pravovye i kriminologicheskie aspekty // Vserossijskij kriminologicheskij zhurnal. 2017. № 3 (11). S. 607–614

