Научная статья
УДК 343.97
DOI: 10.17150/1819-0928.2021.22(3).268-276

Факторы кибервиктимизации

Дмитрий Витальевич Жмуров
Байкальский государственный университет, Иркутск, Россия
zdevraz@ya.ru, https://orcid.org/0000-0003-0493-265X

АННОТАЦИЯ
В статье подробно рассмотрены факторы кибервиктимизации, т. е. причины и движущие силы обозначенного процесса. Проанализированы существующие определения факторов виктимизации и на их основе сформулировано авторское определение применительно к изучаемой тематике. Под факторами кибервиктимизации предлагается понимать существенные обстоятельства (причины и условия) превращения личности в жертву кибернетических преступлений. В ходе метаанализа отечественных и зарубежных исследований выявлено четыре уровня факторов кибервиктимизации, предложена их дефиниция и систематизированы структурные компоненты. Выделены четыре группы виктимогенных триггеров: 1) поведенческие (в форме деятельности индивида, оказывающей влияние на детерминацию виктимных состояний); 2) психологические (выражающиеся в сознательных и бессознательных психических конструктах, определяющих поведение потенциальных жертв в виртуальной среде); 3) социальные (факты жизни общества, коррелирующие с показателями кибервиктимизации); 4) технические (комплекс факторов, относящийся к инфраструктуре, поддерживающей высокотехнологичное развитие общества, и формирующий отраслевые виктимогенные риски). Указанные факторы снабжены подробным описанием и конкретизацией входящих в них субкомпонентов. Кроме того, в статье выполнена визуализация указанной модели методом ментального картирования. Автором сформулированы основные выводы, касающиеся проблемы детерминации кибервиктимного поведения. Во-первых, подчеркивается достаточная диверсифицированность обусловливающих ее фактов. Во-вторых, отмечается, что представленные факторы находятся в постоянной трансформации, а кибервиктимизация критически зависит от них. В-третьих, артикулируется уникальность поведенческих и технических триггеров виртуальной виктимизации. В-четвертых, на обсуждение выносится вопрос о специфичности психологических факторов кибервиктимизации и их отличии от факторов виктимизации традиционной.

КЛЮЧЕВЫЕ СЛОВА
кибервиктимизация, жертвы в интернете, кибервиктимность, кибервиктимология, интернет-потерпевший

ДЛЯ ЦИТИРОВАНИЯ
Жмуров Д.В. Факторы кибервиктимологии // Академический юридический журнал. 2021. Т. 22, № 3. С. 268–276. DOI: 10.17150/1819-0928.2021.22(3).268-276.

Original article

Factors of cyber-victimization

Dmitry V. Zhmurov
Baikal State University, Irkutsk, Russia
zdevraz@ya.ru, https://orcid.org/0000-0003-0493-265X

ABSTRACT
The article discusses in details the factors of cyber-victimization, i. e. reasons and driving forces of the considered process. The author considers the existing definitions of "victimization factors" and, on their basis, his own definition is formulated in relation to the subject of the study. Thus, it is proposed to understand the factors of cyber victimization as the essential circumstances (causes and conditions) of the transformation of an individual into a victim of cybercrimes. In the course of a meta-analysis of domestic and foreign studies, four levels of cyber-victimization factors have been identified, their definition has been proposed, and their structural components have been systematized. It is proposed to distinguish four groups of victimogenic triggers, among them: 1. behavioral (in the form of an individual›s activity that influences the determination of victim states); 2. psychological (which are expressed in conscious and unconscious mental constructs that determine the behavior of potential victims in a virtual environment); 3. social (facts of the society's life, correlating with indicators of cyber-victimization) and 4. technical (as a complex of factors relating to the infrastructure that supports high-tech development of society and forms industry victim-related risks). The specified factors are provided with a detailed description and specification of the subcomponents included in them, in addition, visualization of the

specified model by the method of mental mapping is performed in the article. The author formulates the main findings concerning the problem of determination cyber-victim behavior. First, the sufficient diversity of the underlying facts is emphasized. Secondly, it is noted that the presented factors are in constant transformation, and cyber-victimization critically depends on them. Third, the uniqueness of behavioral and technical triggers of virtual victimization is articulated. Fourth, the question of the specificity of psychological factors of cyber-victimization and the difference between their factors of traditional victimization is brought up for discussion.

KEYWORDS
cyber victimization, victims on the Internet, cyber victimhood, cyber victimology, Internet victim

FOR CITATION
Zhmurov D.V. Factors of cyber-victimization. *Akademicheskiy yuridicheskiy zhurnal = Academic Law Journal.* 2021;22(3):268–276.(In Russ.) DOI: 10.17150/1819-0928.2021.22(3).268-276.

В мировой мифологии сюжет отцеубийства не столь экзотичен. Он встречается в греческой (Эдип, Кронос), вавилонской (Эа), индуистской (Бабрувахана), скандинавской (Фафнир) культурах. Вместе с тем любой миф символичен, и канва его сюжета с некой условностью может отразиться в происходящих сегодня событиях. Мифологические отголоски порождают порой весьма причудливые сравнения. Например, случай с британским ученым Тимом Бернерсом-Ли. В восьмидесятые годы он стал одним из «создателей» Интернета. В двухтысячные – оказался его «жертвой»: стал поживой мошенников, делая онлайн покупки[1]. В некотором смысле, отец-основатель пострадал от собственного детища. Есть в этом своеобразная ирония, драматизм и знакомый сюжет.

На протяжении своего развития человечество не раз оказывалось заложником собственных идей и открытий. Это не только про интернет, но и про ядерное оружие, синтезирование фреона, создание антибиотиков, телекоммуникации и много чего еще. За эти достижения неизбежной была расплата. Динамит, экстази, ядерный распад, виртуальная экзистенция, химические удобрения, ГМО, двигатель внутреннего сгорания – перечень достаточно обширный. Польза от применения этих изобретений всегда шла в союзе с рукотворными катастрофами. Так вышло и с глобальной сетью. Помимо положительных эффектов, она культивировала целый пласт проявлений кибердевиантности, в содержательном поле которой есть особый сегмент, выступающий предметом данной статьи. Речь о кибернетической виктимности, или, по авторскому определению, *способности индивида быть жертвой компьютерных преступлений в силу субъективной или объективной уязвимости*.

Сейчас кибервиктимность и сопутствующая ей виктимизация проходят новые эволюционные циклы: если несколько десятков лет назад виртуальный вред ограничивался исключительно дискриминацией в сфере программного компонента, то ближайшее будущее сулит возможность нанесения физического вреда через глобальную сеть. Уже сейчас вполне осуществимы убийства и причинение вреда здоровью посредством нарушения работы бодинет-устройств (например, кардиостимуляторов, инсулиновых помп, подключенных к Интернету). Футурологи вполне серьезно обсуждают возможность нейрохакинга, т. е. взлома центральной нервной системы человека, который будет технологически достижим в обозримом будущем.

Настоящее исследование посвящено факторам кибервиктимизации, т. е. обстоятельствам, вызывающим реализацию виктимного потенциала. Это тема отражена в различных тематически не пересекающихся публикациях. Несмотря на их разнообразие, один ключевой вопрос звучит повсеместно. Его можно сформулировать следующим образом: какие причины и условия приводят к виктимизации в виртуальном пространстве? Ответов предостаточно, но они нередко затрагивают частные аспекты кибервиктимизации, т. е. изучают формирование жертв отдельных типов посягательств (чаще всего кибербуллинга, интернет-мошенничества, хищения персональной информации, различных форм преследования и пр.).

Вместе с тем очевидна необходимость в построении комплексной модели виктимогенных факторов в интернет-пространстве. Она должна по возможности учитывать все многообразие источников, детерминирующих изучаемое явление. Не исключено, что начало этой работе будет положено в настоящей статье.

Напомним, что под факторами понимаются причины, движущие силы какого-либо процесса, обусловливающие его характер или отдельные черты. При этом факторы виктимизации понимаются по-разному.

Например, К.В. Вишневецкий усматривает в них *совокупность обстоятельств*, детерминирующих или иным образом способствующих процессу превращения личности в жертву преступления [1].

[1] Создатель всемирной паутины стал жертвой интернет-мошенников. URL: https://ria.ru/20090316/165035680.html.

В.В. Вандышев полагает, что этими факторами выступают *свойства личности* (социальные, нравственно-психологические и биофизические), определяющие ту или иную степень ее уязвимости [2].

А.А. Глухова, С.В. Изосимов, А.Е. Шалагин трактуют «виктимологические факторы» шире, понимая под ними *совокупность социальных компонентов*, своеобразную общность личностных качеств и средовых характеристик, обусловливающих состояние виктимизации [3].

Немало авторов разделяют эту позицию, отмечая, что персональные качества жертвы и факторы обстановки являются неотъемлемыми, порой равнозначными элементами, вызывающими виктимизацию [4].

Максимально широкое и абстрактное понимание указанных факторов предлагает А.А. Кулакова, называя ими любые *явления или процессы,* находящиеся в причинной связи с совершенным впоследствии преступлением [5].

Все перечисленные позиции по-своему корректны и отражают многообразие мнений в оценке причинного комплекса виктимизации. Что касается факторов кибервиктимизации, то в сущностном плане они ничем не отличаются от факторов виктимизации. Это точно такие же обстоятельства, которые детерминируют провоцирующее поведение в виртуальном пространстве. Следовательно, меняются лишь место действия, ситуационные риски и набор конкретных виктимогенных обстоятельств. Эти специфические признаки могут находить отражение в частных теориях, не вступая в противоречие с общими положениями виктимологии. Одной из таких разработок является концепция «электронных форм виктимности» Шулера [6].

Итак, факторами кибервиктимизации выступают существенные обстоятельства (причины и условия) превращения личности в жертву кибернетических преступлений. Они могут быть классифицированы по объективным и субъективным основаниям [7], сфере проявления и иным критериям. Не претендуя на универсальность и академическую полноту, предположим, что указанные факторы можно представить несколькими ключевыми позициями, среди которых следует обозначить:

1. ***Поведенческие триггеры,*** оказывающие влияние на детерминацию виктимных состояний. Это организованная деятельность индивида, его конкретные поступки и образ действий, привлекающие внимание со стороны преступных элементов или облегчающие совершение против него уголовно-наказуемого деяния.

Выражается в реализации жертвой неких поведенческих паттернов, повышающих вероятность или провоцирующих совершение в ее отношении дискриминационных актов. Для разных типов виктимизации (например, от кибермошенничества, кибersталкинга, клеветы в социальных сетях и проч.), поведенческие триггеры потерпевшего могут быть совершенно разными. Ключевыми среди них признаются:

– *активное участие в социальных сетях* [8], *высокая онлайн активность* [9], *избыточная увлеченность интернетом* [10]; *участие в онлайн играх* [11];

– *чрезмерная репрезентация личности в сетевом пространстве*, предполагающая пользование широкого спектра цифровых платформ, демонстрацию большого количества персональных данных, личных фотографий, использование геометок при размещении постов и проч.;

– просмотр *порнографических материалов* [12];

– использование *неоднозначных средств виртуальной коммуникации*, например, порнографических онлайн-чатов [13];

– *скачивание пиратских программ*, видео- и аудио контента [14; 15];

– *установка программ и приложений с низким рейтингом* или отрицательными отзывами;

– совершение покупок в интернете, *импульсивное финансовое и «эмоциональное» потребительское поведение* [16; 17];

– *стремление к быстрому и высокому заработку* [7];

– *пренебрежение программами антивирусной защиты*: отказ от их установки либо обслуживания. Установлено, что игнорирование функции обновления защитного софта в 5,5 раз повышает риск заражения компьютера вредоносными программами[2];

– *неосмотрительное и некритичное поведение при использовании электронных устройств*, например, использование общественного Wi-Fi в туристических поездках без должной внимательности (87%)[3]; совершение банковских операций через публичный Wi-Fi; передача конфиденциальной корпоративной информации через открытые сети; отсылка и прием сообщений сексуального характера или *секстинг*; сообщение незнакомым лицам персональных данных; реагирование на сомнительные письма и открытие вложенных в них файлов, использование неизвестных флеш-

[2] Отсутствие антивируса увеличивает вероятность заражения вредоносными программами в 5,5 раз. URL: https://briit.net/it/4840-otsutstvie-antivirusa.html.

[3] Лаборатория Касперского: хакеры атакуют за границей каждого пятого топ-менеджера из РФ. URL: https://tass.ru/ekonomika/3431672.

накопителей, одного пароля для разных сайтов, использование слабых паролей, ответы на фишинговые письма, переходы по коротким ссылкам и доверие QR-ссылкам;

– *удаленная работа на дому* в дистанционном формате[4];

– *демонстрация вербальной агрессии* в процессе интернет-коммуникации (использование нецензурных выражений, стремление реагировать на обидные выражения и агрессию в социальных сетях симметричным образом);

– *виктимная инертность*, т. е. неспособность или нежелание реагировать на действия киберпреступников адекватным образом.

Подобное поведение может расцениваться криминальными элементами, как поощряющее и стимулировать дальнейшее усиление их активности. Проявляется в отсутствии социальных сигналов или прямой обратной связи со стороны жертвы, способных смягчить поведение преступника при кибербуллинге [18], нежелании или отказе потерпевших от преследования «киберпреступников» законными средствами [19] и проч.

Поведенческие триггеры предполагают активное присутствие индивида в сетевом пространстве, чаще всего выраженное в необдуманном (опрометчивом) финансовом, коммуникативном, попустительском поведении.

2. ***Психологические триггеры*** связаны с психической деятельностью личности и ее виктимогенными проявлениями. Выражаются в комплексе сознательных и бессознательных конструктов, определяющих поведение потенциальных жертв. В настоящее время исследователи пытаются индивидуализировать этот механизм применительно к жертвам тех или иных форм виртуальной дискриминации.

Несмотря на предпринимаемые попытки создания единой модели кибержертвы [20], основанной на выделении ядра ее базовых характеристик, вероятно, эти старания не всегда будут успешными и целесообразными.

С одной стороны, это связано с большим количеством киберпотерпевших в популяции, многообразием этой группы и неравномерностью внимания к подгруппам ее составляющим. Жертвы кибербуллинга, например, изучены намного лучше потерпевших от фейков или брачных афер. Логично предположить, что психологические предпосылки виктимного поведения у них будут серьезно отличаться. В этом смысле неоправданно распространять выводы, касающиеся локально исследованной подгруппы жертв на всю когорту интернет-потерпевших.

С другой стороны, отдельные выводы о психологических особенностях пострадавших в виртуальном пространстве (их повышенная тревожность, низкая самооценка, стремление к поиску острых ощущений и т. д.) не означают, что среди невиктимизированных лиц подобных характеристик не наблюдается. Сегодня нет данных, позволяющих наверняка утверждать, что кибержертвы по своим психологическим свойствам отличаются от «обычных» людей. И тем, и другим свойственны все обнаруживаемые признаки.

Среди таковых выделяют:

– *симптомокомплекс виртуальной жертвы* (беспокойство, неуверенность в себе, подверженность настроению, неусидчивость, неустойчивость настроения, гневливость) [20];

– *высокие баллы по шкале нейротизма, открытость, антисоциальное поведение, застенчивость, отстраненность, психопатологические расстройства* [21]. Любопытно, но киберагрессоры в данном исследовании испанской молодежи демонстрировали схожие черты и качества;

– *установка на рискованное социальное поведение, конформность, тревожность, интроверсия, склонность к зависимому и беспомощному поведению*, высокая чувствительность, потребность в поддержке и сочувствии [10];

– *посттравматические и стрессовые реакции*, в том числе опыт виктимизации в реальной жизни и долговременные психологические проблемы [22];

– *внушаемость, доверчивость, неосмотрительность, отсутствие критического мышления, беспечность* [7; 23];

– отдельная группа *качеств, связанных с функционированием индивида в условиях виртуальной реальности и погружением в нее*. В нее входят:

• *виртуализация сознания*, как тенденция включаться в виртуальную коммуникативную среду вплоть до полной или частичной утраты собственной идентичности;

• *кибер-аутизация* – уход от реальности в мир виртуальных переживаний, предпочтение виртуальных средств общения реальным и проч. В современной науке этот феномен только начал изучаться и получил обозначение «цифровой аутизм». Исследования британских ученых свидетельствуют о том, что человек в среднем совершает 76 сессий со смартфоном ежедневно и это, безусловно, не может не сказываться на его фак-

[4] Киберпреступность и Covid-19: риски и ответные меры : аналит. докл. // UNODC Report. Вена, 2020. 14 апр. URL: https://мвд.рф/upload/site151/doc/UPN_OON._Doklad_Prestupnost_i_Covid.pdf.

тической деятельности, концентрации на реальном бытии[5];

• *виктимная амбивалентность* – высокая представленность среди кибержертв тех, кто допускает противоправное и аморальное поведение, провоцируя тем самым преступления в отношении себя;

• *психологические особенности киберсерфинга и виктимная дезингибиция* (мнимое ощущение психологической защищенности перед компьютером, в знакомой обстановке, впечатление нереальности происходящего, позволяющее чувствовать себя менее ответственным за собственные действия).

3. ***Социальные триггеры*** связаны с жизнью людей в обществе, их отношениями в группах и между собой.

Это социальные факты, коррелирующие с показателями кибервиктимизации. Накопленные знания о содержании данных «спусковых механизмов» пока не отражают всю широту и сложность социальных условий. Из факторов, которые уже упоминались учеными в гипотетической связи с виртуальной виктимизацией, можно упомянуть следующие:

– *подавляющая компьютеризация и цифровизация*, развитие телекоммуникационной инфраструктуры, стремящейся к одним и тем же параметрам: растущему охвату сотовой связи и доступа в Интернет [24]. Сменяющие друг друга технологические уклады VUCA-мира, когда люди становятся заложниками дигитальных технологий, теряют навыки или физические возможности альтернативных (аналоговых) форм активности. При этом роль информационно-коммуникационных технологий возрастает критически и значительная часть повседневных функций, потребностей, интересов переходит в виртуальный мир;

– все большее *включение персональных данных частных лиц и организаций* в различные информационные системы для расширения сферы оказания различных услуг [7]. Объем персональных данных демонстрирует лавинообразный рост, как и величина их утечек. В 2020 году, по данным компании Infowatch, в глобальной сети было скомпрометировано 11 миллиардов записей персональных данных, в России – около 100 миллионов. Чаще всего утечки происходили в хайтек-индустрии, финансовой сфере и государственном секторе[6];

– *умеренное (фактически минимальное) вмешательство государственных органов* и должностных лиц в сферу функционирования информационно-коммуникационных технологий, обусловленное необходимостью соблюдения прав гражданина на свободное получение и распространение информации любым законным способом [7];

– *формирование в обществе культурных взглядов, связанных с поощрением самопрезентации собственного «*Я*»* в виртуальном пространстве. Критерием самовыражения и самореализации становится активное поведение в социальных сетях, создание блогов, Инстаграм или Тик-ток аккаунтов и участие в них, т. е. коммуникационные нормы, поощряющие *цифровой вуайеризм;*

– *невысокий уровень компьютерной грамотности,* предполагающий отсутствие у большинства населения цифровых компетенций, обеспечивающих должный уровень интернет-безопасности, ответственного, дозированного и субъективно-контролируемого использования возможностей мировой сети, дефицит компетенций фактчекинга, т. е. умения отбирать проверенную информацию [25];

– *цифровая миграция преступности*, т. е. смещение значительного объема криминальной активности в виртуальную среду, а вред, наносимый ею, уже оценивается как «крайне существенный» [26];

– возможные *социальные проблемы в микросреде кибержертв*. Так, ряд исследователей при изучении кибербуллинга обращают внимание на факторы семейной неустроенности потерпевших, низкий образовательный уровень в родительской семье и т. д. В частности, высказываются мнения о том, что онлайн виктимизация тесно связана с проблемами семейной привязанности [9], низким и выше среднего уровнем образования родителей [27], отсутствием сплоченности, обедненными эмоциональными связями между членами семьи, ее структурной неполнотой [28], ослабленным родительским контролем [29].

4. ***Технические триггеры*** – комплекс факторов, относящийся к инфраструктуре, поддерживающей высокотехнологичное развитие общества, и формирующий отраслевые виктимогенные риски. Этот комплекс получил название «виктимность компьютера» (В. А. Бессонов [30]). Речь в данном случае идет о следующих немаловажных моментах:

– *несовершенство и уязвимости компьютерных систем*, непредвиденные или заложенные программные ошибки; опасности, связанные с дистанционным обслуживанием компьютеров и проч.;

[5] Доктор Курпатов рассказал о влиянии интернета на мозг. URL: https://news.myseldon.com/ru/news/index/222105557.

[6] Эксперты оценили объем «утечек» персональных данных россиян в 2020 году. URL: https://www.vedomosti.ru/technology/news/2021/01/11/853607-eksperti-otsenili-obem-utechek-personalnih-dannih-rossiyan-v-2020-godu.

– *технические риски, связанные с работой оборудования* (сбои в связи с природными и техногенными катастрофами, незащищенное хранение информации и неконтролируемое копирование, недостаточное обслуживание и обучение персонала безопасности, неконтролируемая работа внешним штатом, низкий уровень менеджмента паролей, недоработанное или новое программное обеспечение, незащищенная сетевая инфраструктура, неправильное распределение прав доступа и т. п.);

– *технократические изменения*, используемые для повышения комфорта коммуникации, юзабилити гаджетов и персональных устройств, *создающие побочные виктимогенные риски* (тотальная предустановка веб-камер на цифровые устройства, использование систем геолокации по умолчанию, контроль показателей здоровья посредством цифрового оборудования, т. е. все «достижения» и «удобства», которые могут быть использованы в целях компрометации);

– *ориентация на техноценоз,* т. е. стремление производителей к созданию цифровых экосистем, когда все домашние, рабочие или корпоративные устройства объединяются в единые сети. Нарушение работы или взлом любого из включенных в эту систему устройств угрожает жизнеспособности всего технического организма;

– *виктимогенные тренды в цифровой сфере*, предлагаемые неопределенно большому числу пользователей. Например, внедрение практик сквозной авторизации, создания мастер-паролей, эксплуатации хранилищ паролей, ассоциированных с браузерами, хранения данных платежных карт на компьютере и т. д.;

– *техническая дезадаптация* значительного числа участников цифрового мира. Она связана со сложностями приспособления людей к беспрерывно обновляющимся цифровым устройствам и сменяющим друг друга технологиям. Эту драматическую ситуацию можно обозначить термином «*цифровая растерянность*», когда современный человек не успевает привыкнуть к вновь возникающим, стремительно эволюционирующим техническим реалиям.

Таким образом, кибервиктимизация является результатом действия всех вышеупомянутых триггеров: поведенческих, психологических, социальных, технических.

Визуально это тетраду факторов можно проиллюстрировать следующим образом (рис. 1).

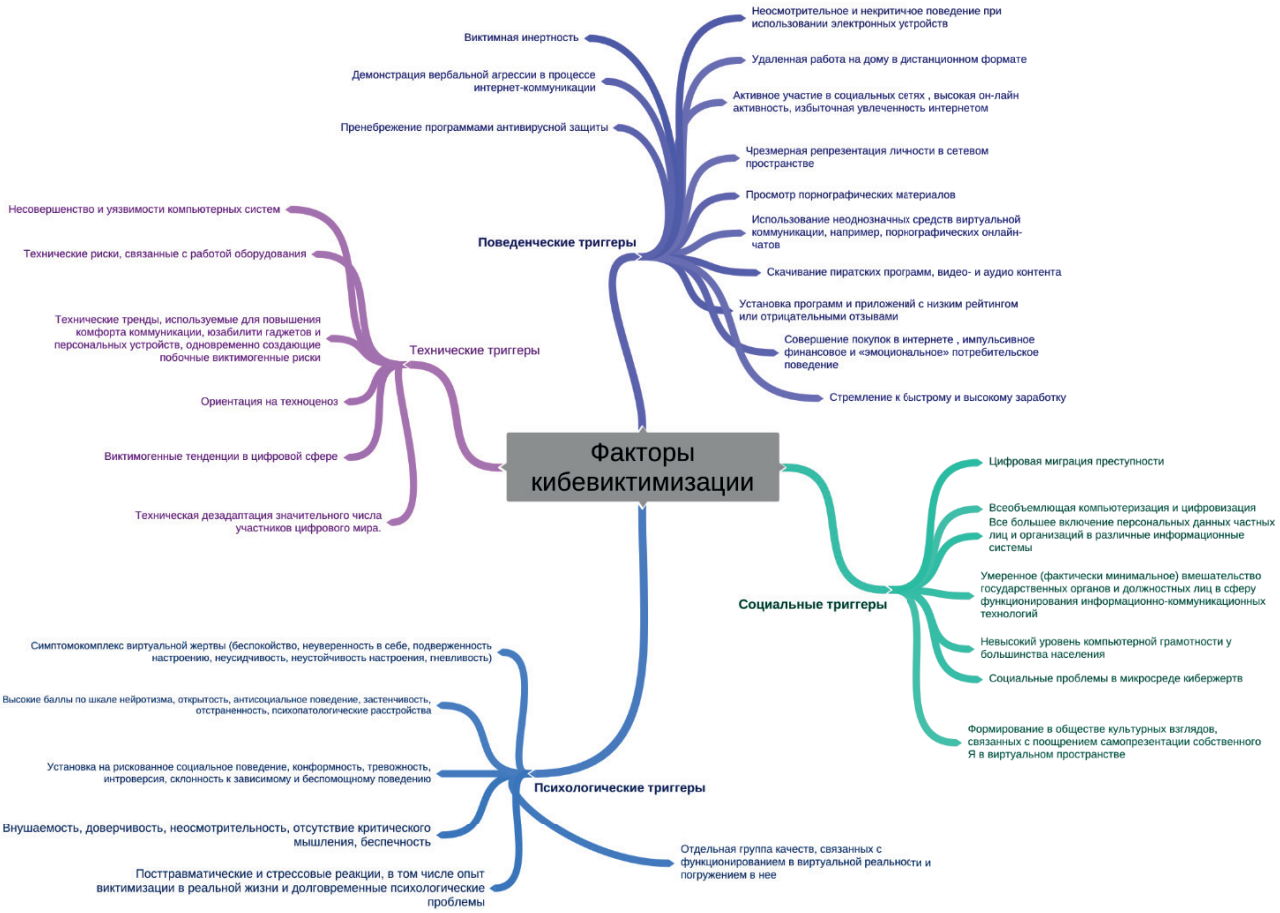

Рис. 1. Ментальная карта факторов кибервиктимизации

В заключение хотелось бы отметить гипотетическую природу указанных факторов, их разнообразие и несопоставимость. Это означает, что научные исследования в данной области находятся в самом начале пути, происходит первичное накопление эмпирического материала, по результатам которого предстоит сделать серьезные научные выводы. Однако это не означает, что отдельные умозаключения не могут быть сформулированы сейчас.

Во-первых, очевидно, что факторы кибервиктимизации достаточно диверсифицированы. Они представлены в единстве четырех взаимосвязанных компонентов: культурного, технического, психологического и поведенческого.

Во-вторых, представленные факторы находятся в постоянной трансформации, кибервиктимизация ведома ими, она эволюционирует вслед за изменением указанных причин и условий.

В-третьих, специфика виртуального бытия накладывает свой отпечаток на процесс виктимизации в интернете, особенно в части уникальности поведенческих и технических триггеров.

В-четвертых, в разрешении нуждается вопрос о психологических факторах кибервиктимизации и их негативном потенциале, а именно: являются ли эти факторы уникальными для кибержертв и не присущими остальному большинству населения.

СПИСОК ИСТОЧНИКОВ

1. Вишневецкий К.В. Виктимизация: факторы, условия, уровни / К.В. Вишневецкий // Теория и практика общественного развития. – 2014. – № 4. – С. 226–227.

2. Вандышев В.В. Изучение личности потерпевшего в процессе расследования / В.В. Вандышев. – Ленинград : Изд-во ВПУ МВД СССР : Изд-во ЛВК МВД СССР, 1989. – 92 с.

3. Шалагин А.Е. Криминальная виктимология: понятие, содержание, профилактика / А.Е. Шалагин // Вестник Казанского юридического института МВД России. – 2017. – № 1 (27). – С. 62–65.

4. Ахмедшина Н.В. Механизм взаимодействия между жертвой преступления и преступником / Н.В. Ахмедшина. – DOI 10.17223/15617793/413/26 // Вестник Томского государственного университета. – 2016. – № 413. – С. 172–176.

5. Кулакова А.А. Виктимологический аспект пенитенциарной преступности и ее предупреждения (в отношении сотрудников уголовно-исполнительной системы) : автореф. дис. ... канд. юрид. наук : 12.00.08 / А.А. Кулакова. – Нижний Новгород, 2007. – 23 с.

6. Suler J. The Online Disinhibition Effect / J. Suler. – DOI 10.1089/1094931041291295 // Cyberpsychology & Behavior: the Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society. – 2004. – Vol. 7, iss. 3. – P. 321–326.

7. Жакупжанов А.О. Виктимологические факторы киберпреступности / А.О. Жакупжанов // Алтайский юридический вестник. – 2019. – № 3 (27). – С. 75–82.

8. Алексеева Е.А. Активное участие в социальных интернет-сетях как новый фактор виктимности лиц, в отношении которых совершаются кражи с незаконным проникновением в жилище / Е.А. Алексеева // Вестник Курганского государственного университета. Серия: Гуманитарные науки. – 2014. – № 3 (34). – С. 3–6.

9. Cyberbullying Victimization at Work: Social Media Identity Bubble Approach / A. Oksanen, R. Oksa, N. Savela [et al.]. – DOI 10.1016/j.chb.2020.106363 // Computers in Human Behavior. – 2020. – Vol. 109. – P. 106363.

10. 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.

11. Комаров А.А. Виктимологические аспекты интернет-мошенничества / А.А. Комаров // Тенденции и противоречия развития российского права на современном этапе : сб. ст. VIII Всерос. науч.-практ. конф. – Пенза, 2009. – С. 156–159.

12. Buzzell T. Explaining use of Online Pornography: A Test of Self-Control Theory and Opportunity for Deviance / T. Buzzell, D. Foss, Z. Middleton // Journal of Criminal Justice and Popular Culture. – 2006. – Vol. 13, iss. 2. – P. 96–116.

13. Hinduja S. Cyberbullying: An Exploratory Analysis of Factors Related to Offending and Victimization / S. Hinduja, J.W. Patchin. – DOI 10.1080/01639620701457816 // Deviant Behavior. – 2008. – Vol. 29, iss. 2. – P. 129–156.

14. Exploring the Link between Low Self-Control and Violent Victimization Ttrajectories in Adolescents / G.E. Higgins, W.G. Jennings, R. Tewksbury, C.L. Gibson. – DOI 10.1177/0093854809344046 // Criminal Justice and Behavior. – 2009. – Vol. 36, iss. 10, – P. 1070–1084.

15. Moon B. A General Theory of Crime and Computer Crime: An Empirical Test / B. Moon, J. Mccluskey, C.P. Mccluskey. – DOI 10.1016/j.jcrimjus.2010.05.003 // Journal of Criminal Justice. – 2010. – Vol. 38, iss. 4. – P. 767–772.

16. Self-Control, Violent Offending, and Homicide Victimization: Assessing the General Theory of Crime / A.R. Piquero, J. MacDonald, A. Dobrin [et al.]. – DOI 10.1007/s10940-004-1787-2 // Journal of Quantitative Criminology. – 2005. – Vol. 21, iss. 1. – P. 55–71.

17. Reisig M.D. Perceived Risk of Internet Theft Victimization: Examining the Effects of Social Vulnerability and Financial Impulsivity / M.D. Reisig, T.C. Pratt, K. Holtfreter. – DOI 10.1177/0093854808329405 // Criminology and Criminal Justice. – 2009. – Vol. 36, iss. 4. – P. 369–384.

18. Макарова Е.А. Психологические особенности кибербуллинга как формы интернет-преступления / Е.А. Макарова, Е.Л. Макарова, Е.А. Махрина. – DOI 10.21702/rpj.2016.3.17 // Российский психологический журнал. – 2016. – Т. 13, № 3. – С. 293–311.

19. Скурихина А.А. Виктимность в сфере компьютерных преступлений / А.А. Скурихина, О.С. Ронжина // Виктимология. – 2014. – № 2 (2). – С. 47–50.

20. Сафуанов Ф.С. Особенности личности жертв противоправных посягательств в Интернете / Ф.С. Сафуанов, Н.В. Докучаева. – DOI 10.17759/psylaw.2015050407 // Психология и право. – 2015. – Т. 5, № 4. – С. 80–93.

21. Garaigordobil M. Psychometric Properties of the Cyberbullying Test, a Screening Instrument to Measure Cybervictimization, Cyberaggression, and Cyberobservation / M. Garaigordobil. – DOI 10.1177/0886260515600165 // Journal of Interpersonal Violence. – 2015. – Vol. 30, iss. 23. – P. 3556–3576.

22. Duan W. Relationships among Trait Resilience, Virtues, Post-Traumatic Stress Disorder, and Posttraumatic Growth / W. Duan, P. Guo, P. Gan. – DOI 10.1371/journal.pone.0125707 // PLoS ONE. – 2015. – Vol. 10, iss. 5. – P. e0125707.

23. Антонян Е.А. Кибервиктимность / Е.А. Антонян, Е.Н. Клещина // Вестник Пермского института ФСИН России. – 2019. – № 3 (34). – С. 5–10.

24. Болданова Е.В. Тенденции в мировых телекоммуникациях / Е.В. Болданова. – DOI 10.17150/2411-6262.2017.8(1).11 // Baikal Research Journal. – 2017. – Т. 8, № 1. – URL: http://brj-bguep.ru/reader/article.aspx?id=21385.

25. Фактчекинг и верификация информации в контексте журналистского образования / Л.П. Шестеркина, Л.К. Лободенко, А.В. Красавина, А.Р. Марфицына. – DOI 10.17150/2308-6203.2021.10(1).94–108 // Вопросы теории и практики журналистики. – 2021. – Т. 10, № 1. – С. 94–108.

26. Гладких В. И. Проблемы совершенствования уголовно-правовых мер противодействия преступлениям в сфере компьютерной информации / В.И. Гладких, И.Н. Мосечкин. – DOI 10.17150/2500-4255.2021.15(2).229-237 // Всероссийский криминологический журнал. – 2021. – Т. 15, № 2. – С. 229–237.

27. Cyberbullying Victimization Prevalence and Associations with Internalizing and Externalizing Problems among Adolescents in six European Countries / A. Tsitsika, M. Janikian, S. Wójcik [et al.]. – DOI 10.1016/j.chb.2015.04.048 // Computers in Human Behavior. – 2015. – Vol. 51. – P. 1–7.

28. Sasson H. Parental Mediation, Peer Norms and Risky Online Behaviors among Adolescents / H. Sasson, G.S. Mesch. – DOI 10.1016/j.chb.2013.12.025 // Computers in Human Behavior. – 2014. – Vol. 33. – P. 32–38.

29. Vakhitova Z. Toward the Adaptation of Routine Activity and Lifestyle Exposure Theories to Account for Cyber Abuse Victimization / Z. Vakhitova, D. Reynald, M.K. Townsley. – DOI 10.1177/1043986215621379 // Journal of Contemporary Criminal Justice. – 2015. – Vol. 32, iss. 2. – P. 169–188.

30. Бессонов В.А. Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации : автореф. дис. ... канд. юрид. наук : 12.00.08 / В.А. Бессонов. – Нижний Новгород, 2000. – 28 с.

REFERENCES

1. Vishnevetskiy K.V. Victimization: Factors, Conditions, Levels. *Teoriya i praktika obshchestvennogo razvitiya = Theory and Ppractice of Social Development,* 2014, no. 4, pp. 226–227. (In Russian).

2. Vandyshev V.V. *The Study of the Personality of the Victim during the Investigation*. Leningrad, Voenno-Politicheskoe uchilishche MVD SSSR Publ., 1989. 92 p.

3. Shalagin A.E. Criminal Victimology: Concept, Contents and Prevention. *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii = Bulletin of the Kazan Law Institute of MIA Russia,* 2017, no. 1, pp. 62–65. (In Russian).

4. Akhmedshina N.V. The Mechanism of Interaction between the Victim of the Crime and the Criminal. *Vestnik Tomskogo gosudarstvennogo universiteta = Tomsk State University Journal*, 2016, no. 413, pp. 172–176. (In Russian). DOI: 10.17223/15617793/413/26.

5. Kulakova A.A. *Victimological Aspect of Penitentiary Crime and its Prevention (in Relation to Employees of the Penitentiary system). Cand. Diss. Thesis.* Nizhny Novgorod, 2007. 23 p.

6. Suler J. The Online Disinhibition Effect. *Cyberpsychology & Behavior: the Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society,* 2004, vol. 7, iss. 3, pp. 321–326. DOI:10.1089/1094931041291295.

7. Zhakupzhanov A.O. Victimological Factors of Cybercrime. *Altaiskii yuridicheskii vestnik = Altai Law Journal,* 2019, no. 3, pp. 75–82. (In Russian).

8. Alekseeva E.A. Active Participation in Social Internet Networks as a New Factor of Victimization of Persons Against whom Theft with Illegal Entry into a Dwelling is Committed. *Vestnik Kurganskogo gosudarstvennogo universiteta. Seriya: Gumanitarnye nauki = Vestnik of the Kurgan State University. Series: Humanities,* 2014, no. 3, pp. 3–6. (In Russian).

9. Oksanen A., Oksa R., Savela N., Kaakinen M., Ellonen N. Cyberbullying Victimization at Work: Social Media Identity Bubble Approach. *Computers in Human Behavior*, 2020, vol. 109, pp. 106363. DOI: 10.1016/j.chb.2020.106363.

10. Drozdikova-Zaripova A.R., Kalatskaya N.N., Valeeva R.A., Kostyunina N.Yu., Biktagirova G.F. Socio-Psychological Features of Students Inclined to Victim Behavior in the Internet. *Sovremennye naukoemkie tekhnologii= Modern High Technologies,* 2019, no. 12, pt. 1, pp. 159–166. (In Russian). DOI: 10.17513/snt.37852.

11. Komarov A.A. Victimological Aspects of Internet-Fraud. In *Trends and Contradictions in the Development of Russian Law at the Present Stage. Collected Papers Based on the Materials of the 8th All-Russian Scientific and Practical Conference*. Penza, 2009, pp. 156–159. (In Russian).

12. Buzzell T., Foss D., Middleton Z. Explaining use of Online Pornography: A Test of Self-Control Theory and Opportunity for Deviance. *Journal of Criminal Justice and Popular Culture,* 2006, vol. 13, iss. 2, pp. 96–116.

13. Hinduja S., Patchin J.W. Cyberbullying: An Exploratory Analysis of Factors Related to Offending and Victimization. *Deviant Behavior*, 2008, vol. 29, iss. 2, pp. 129–156. DOI:10.1080/01639620701457816.

14. Higgins G.E., Jennings W.G., Tewksbury R., Gibson C.L. Exploring the Link between Low Self-Control and Violent Victimization Ttrajectories in Adolescents. *Criminal Justice and Behavior*, 2009, vol. 36, iss. 10, pp. 1070–1084. DOI:10.1177/0093854809344046.

15. Moon B., Mccluskey J., Mccluskey C.P. A General Theory of Crime and Computer Crime: An Empirical Test. *Journal of Criminal Justice*, 2010, vol. 38, iss. 4, pp. 767–772. DOI: 10.1016/j.jcrimjus.2010.05.003.

16. Piquero A.R., MacDonald J., Dobrin A., Daigle L.E., Cullen F.T. Self-Control, Violent Offending, and Homicide Victimization: Assessing the General Theory of Crime. *Journal of Quantitative Criminology,* 2005, vol. 21, iss. 1, pp. 55–71. DOI:10.1007/s10940-004-1787-2.

17. Reisig M.D., Pratt T.C., Holtfreter K. Perceived Risk of Internet Theft Victimization: Examining the Effects of Social Vulnerability and Financial Impulsivity. *Criminology and Criminal Justice,* 2009, vol. 36, iss. 4, pp. 369–384. DOI:10.1177/0093854808329405.

18. Makarova E.A., Makarova E.L., Mahrina E.A. Psychological Features of Cyberbullying as a Form of Internet Crime. *Rossiiskii psikhologicheskii zhurnal = Russian Psychological Journal,* 2016, vol. 13, no. 3, pp. 293–311. (In Russian). DOI: 10.21702/rpj.2016.3.17.

19. Skurihina A.A., Ronzhina O.S. Victimization in the Sphere of Computer Crimes. *Viktimologiya = Victimology,* 2014, no. 2, pp. 47–50. (In Russian).

20. Safuanov F.S., Dokuchaeva N.V. Personality Characteristics of Victims of Illegal Attacks on the Internet. *Psikhologiya i pravo = Psychology and Law*, 2015, vol. 5, no. 4, pp. 80–93. (In Russian). DOI: 10.17759/psylaw.2015050407.

21. Garaigordobil M. Psychometric Properties of the Cyberbullying Test, a Screening Instrument to Measure Cybervictimization, Cyberaggression, and Cyberobservation. *Journal of Interpersonal Violence,* 2015, vol. 30, iss. 23, pp. 3556–3576. DOI:10.1177/0886260515600165.

22. Duan W., Guo P., Gan P. Relationships among Trait Resilience, Virtues, Post-Traumatic Stress Disorder, and Posttraumatic Growth. *PLoS ONE,* 2015, vol. 10, iss. 5, pp. e0125707. DOI: 10.1371/journal.pone.0125707.

23. Antonyan E.A., Kleshchina E.N. Cyber Visibility. *Vestnik Permskogo instituta FSIN Rossii = Vestnik of Perm Institute of the Federal Penal Service,* 2019, no. 3, pp. 5–10. (In Russian).

24. Boldanova E.V. Trends in World Telecommunications. *Baikal Research Journal*, 2017, vol. 8, no. 1. Available at: http://brj-bguep.ru/reader/article.aspx?id=21385. (In Russian). DOI: 10.17150/2411-6262.2017.8(1).11.

25. Shesterkina L.P., Lobodenko L.K., Krasavina A.V., Marfitsyna A.R. Fact-Checking and Information Verification in the Context of Journalism Education. *Voprosy teorii i praktiki zhur_nalistiki = Theoretical and Practical Issues of Journalism*, 2021, vol. 10, no. 1, pp. 94–108. (In Russian). DOI: 10.17150/2308-6203.2021.10(1).94-108.

26. Gladkikh .I., Mosechkin I.N. Problems of Improving Criminal Law Measures of Counteracting Crimes in the Sphere of Computer Information. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2021, vol. 15, no. 2, pp. 229–237. (In Russian). DOI: 10.17150/2500-4255.2021.15(2).229-237.

27. Tsitsika A., Janikian M., Wójcik S., Makaruk K., Tzavela E., Tzavara C., Richardson C. Cyberbullying Victimization Prevalence and Associations with Internalizing and Externalizing Problems among Adolescents in six European Countries. *Computers in Human Behavior,* 2015, vol. 51, pp. 1–7. DOI: 10.1016/j.chb.2015.04.048.

28. Sasson H., Mesch G.S. Parental Mediation, Peer Norms and Risky Online Behaviors among Adolescents. *Computers in Human Behavior,* 2014, vol. 33, pp. 32–38. DOI: 10.1016/j.chb.2013.12.025.

29. Vakhitova Z., Reynald D., Townsley M.K. Toward the Adaptation of Routine Activity and Lifestyle Exposure Theories to Account for Cyber Abuse Victimization. *Journal of Contemporary Criminal Justice,* 2015, vol. 32, iss. 2, pp. 169–188. DOI:10.1177/1043986215621379.

30. Bessonov V.A. *Victimological Aspects of Cybercrime Prevention. Cand. Diss. Thesis*. Nizhny Novgorod, 2000. 28 p.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Жмуров Дмитрий Витальевич – кандидат юридических наук, доцент, доцент кафедры уголовного права и криминологии Института юстиции, координатор проекта «Национальная энциклопедическая служба России». Байкальский государственный университет. 664003, Россия, Иркутск, ул. Ленина, 11, Scopus Author ID: 35770006500

INFORMATION ABOUT THE AUTHOR

Dmitriy V. Zhmurov – Ph. D. in Law, Ass. Professor, Ass. Professor, Chair of Criminal Law, Criminology, Institute of Justice, Coordinator of Project «National Encyclopedic Service of Russia». Baikal State University. 11, Lenin st., Irkutsk, 664003, Russia, Scopus Author ID: 35770006500

Поступила в редакцию / Received 09.06.2021

Доработана после рецензирования / Revised 30.08.2021

Принята к публикации / Accepted 20.10.2021