Научная статья
УДК 343.988
EDN ROGYBP
DOI 10.17150/2411-6262.2022.13(1).29

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

КИБЕРВИКТИМОЛОГИЯ. МЕТОДЫ И МЕТРИКА

АННОТАЦИЯ. В статье предложены авторские методы оценки виктимного потенциала индивида в сети Интернет. Под настоящими методами подразумеваются определенные приемы познания и практической деятельности, направленной на выявление двух наиважнейших факторов: во-первых, частоты и опыта кибервиктимизации, имеющихся у индивида (ретроспективный уровень познания); во-вторых, степени его нереализованных виктимных возможностей (перспективный уровень познания). Для указанных целей разработаны соответствующие диагностические инструменты: а) виктимологический опросник интернет-жертв; и б) шкала кибервиктимизации. Первый нацелен на описание фактов виктимизации в интернет-пространстве, их фиксацию и констатацию. Опросник представляет собой максимально расширенный перечень форм и видов кибервиктимизации из которых респондент может выбрать пережитые им лично. Второй инструмент представляет собой тестовую методику диагностики имеющихся виктимогенных тенденций, которые могут быть реализованы в будущем. Тест выполнен в форме стандартизованного задания, охватывающего 4 субшкалы (провоцирующее поведение в интернете, защитные стратегии, цифровая погруженность, опыт кибервиктимизации). Ответ на каждый из вопросов дифференцирован по степени глубины виктимности носителя, начиная от повышенной и заканчивая степенью близкой к нулевой.

КЛЮЧЕВЫЕ СЛОВА. Кибервиктимология, жертвы в цифровом пространстве, кибервиктимность, кибервиктимизация, интернет-жертвы, методы кибервиктимологии.

ИНФОРМАЦИЯ О СТАТЬЕ. Дата поступления 10 января 2022 г.; дата принятия к печати 21 марта 2022 г.; дата онлайн-размещения 30 апреля 2022 г.

Original article

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

CYBERVICTIMOLOGY. METHODS AND METRICS

ABSTRACT. The article suggests the author's methods of assessing the victim's potential of an individual on the Internet. These methods mean certain cognitive techniques and practical activities aimed at identifying two most important factors: firstly, the frequency and experience of cybervictimization an individual has (the retrospective level of cognition); secondly, the degree of the unrealized victim possibilities (the prospective level of cognition). For these purposes, appropriate diagnostic tools have been developed: a) a victimological questionnaire of Internet victims; and b) a scale of cybervictimization. The first one is aimed at describing facts of victimization in the Internet space, their registering and stating. The questionnaire is the fullest possible list of forms and types of cybervictimization from which the respondent can choose the ones he personally experienced. The second tool is a test method for diagnosing existing victimogenic trends that can be implemented in the future. The test was completed in the form of a standardized task covering four subscales (provoking behavior on the Internet, defensive strategies, digital immersion, and experience of cybervictimization). The answer to each of the questions is differentiated by the degree of depth of victimization of the individual, ranging from the highest degree to the degree close to zero.

KEYWORDS. Cybervictimology, victims in the digital space, cybervictimization, cybervictimity, internet victims, methods of cybervictimology.
ARTICLE INFO. Received January 10, 2022; accepted March 21, 2022; available online April 30, 2022.

Методы и методология важны для любой науки. «Уж лучше совсем не помышлять об отыскании каких бы то ни было истин, чем делать это без всякого метода», замечал Р. Декарт. Кибервиктимология, как относительно молодое направление исследований, не является исключением и требует применения строго формализованных, верифицируемых приемов получения информации. Осложняет ситуацию практически полное отсутствие в рассматриваемой области каких-бы то ни было зарекомендовавших себя способов исследования. Более того, задача умелого применения методов виктимологической профилактики [1] в интернете невыполнима без идентификации того контингента, кому они непосредственно должны быть адресованы. Нельзя забывать о том, что виктимность и безопасность представляют собой парные (диалектически единые) категории [2], поэтому разработка методов кибервиктимологии, в конечном итоге, преследует цели обеспечения информационной безопасности граждан.

По всей вероятности, методологическую базу кибервиктимологии можно представить, как совокупность научных инструментов нескольких уровней, среди которых следует обозначить:

– *ретроспективный* (нацелен на резюмирование факта виктимизации в интернет-пространстве, его фиксацию и констатацию, как уже произошедшего события, т.е. имеется ввиду фактографическая сторона вопроса);

– *перспективный* (направлен на выявление имеющихся виктимогенных тенденций, возможностей и шансов кибервиктимизации, которые еще не реализованы. В этом смысле целесообразно говорить о маркерах или предвестниках кибервиктимного поведения).

Таким образом, в первом случае речь идет о социологическом инструментарии, в частности, **виктимологическом опроснике**, цель которого представить респонденту максимально полный перечень форм цифровой дискриминации с просьбой определить (вспомнить) реально пережитые из них.

Во втором случае предполагается разработка диагностического теста или **«шкалы кибервиктимизации»**, благодаря которой можно будет оценить нереализованный виктимный потенциал субъекта при использовании им цифровых средств коммуникации.

Вместе с тем, следует иметь в виду, что данные диагностические методики со времен могут и должны быть автоматизированы. Подобные разработки уже имеются и являются весьма перспективными. Целесообразность подобного подхода обсуждалась в одной из ранних авторских работ.

Итак, приведем указанные методологические инструменты.

1. Виктимологический опросник интернет-жертв

а. Ваш пол: М Ж

б. Ваш возраст: до 18; 19–35; 36–50; 51 и старше

в. Пожалуйста, вспомните какие «неприятные» инциденты случались с Вами в Интернете за последний год:

Угрозы

□ причинения телесных повреждений
□ порчи имущества
□ распространения порочащей информации
□ причинения вреда близким
□ вербальные угрозы общего характера

□ свой вариант: _____

Преследование

□ непристойные шутки
□ сексуальные приставания и домогательства
□ вредоносные розыгрыши
□ спам
□ издевательства на форумах
□ нежелательные и нетактичные комментарии
□ травля за убеждения и взгляды
□ свой вариант: _____

Незаконный интерес

□ шпионаж за моей личной жизнью
□ сбор информации обо мне
□ отслеживание онлайн активности
□ свой вариант: _____

Ущемление

□ демонстративный отказ от общения со мной
□ коллективное игнорирование
□ исключение из онлайн-игр, занятий или дружеских групп
□ необоснованный отказ в реализации моих прав (отключение аккаунта, невозврат средств, пресечение активности)
□ свой вариант: _____

Приписывание

□ клеветнические измышления обо мне
□ распространение слухов
□ ложные обвинения в чем-либо
□ обвинения в непрофессионализме, моей некомпетентности
□ навешивание «ярлыков»
□ ложное цитирование моих слов
□ свой вариант: _____

Оскорбление

□ единичные оскорбления
□ организация оскорбительных опросов и голосований
□ унизительные комментарии
□ уничижительный видеоконтент, посты и проч.
□ свой вариант: _____

Подмена

□ незаконное использование моих фотографий в социальных сетях
□ рассылка писем от моего имени
□ создание в фотошопе компрометирующих меня фотографий
□ обращение в кредитные, страховые и иные организации от моего имени
□ мое общение и деловые контакты с подставным лицом
□ фальсификация информации, повлекшая ущерб для меня
□ продажа мне фальсифицированных товаров
□ свой вариант: _____

Разглашение

□ распространение частной информации обо мне без разрешения
□ публикация моих откровенных фотографий или видео
□ свой вариант: _____

Внушение

□ пропаганда разрушительных и деструктивных идей

□ развращение и совращение
□ пропаганда наркотиков, алкоголя, рискованных поступков
□ пропаганда идей ненависти (хейтерство)
□ навязывание радикальных политических взглядов, призывы к неповиновению и беспорядкам
□ популяризация опасных методов лечения, рискованных форм воздействия на свое тело
□ пропаганда опасных для жизни видов спорта
□ подстрекательство к насилию над собой
□ обесценивание позитивных институтов (семья, родина, долг)
□ свой вариант: _____

Изъятие

□ кража денег, электронных валют, ценных бумаг
□ воровство конфиденциальных данных (паролей, цифровой идентичности, платежной информации)
□ хищение путем обмана (ложное трудоустройство, попрошайничество, лотереи, инвестиции в «пирамиды», обман в интернет-магазинах и прочие виды мошенничества)
□ оплата услуг без моего согласия (платные подписки, списания средств при СМС-подтверждении)
□ вымогательство денежных средств
□ хищение интеллектуальной собственности и нарушение авторских прав
□ нелегальное использование моего интернет-траффика
□ кража бонусных баллов в программах лояльности
□ свой вариант: _____

Заражение

□ заражение моего компьютера вредоносными программами
□ нарушение работы цифровых устройств (программы блокировщики, шифровальщики и т.д.)
□ хакерские атаки на мои гаджеты
□ свой вариант: _____

Доступ

□ взлом моего почтового ящика или аккаунта в социальных сетях
□ удаленный захват управления над моим компьютером
□ просьбы под разными предлогами перейти или зарегистрироваться на сомнительных сайтах
□ свой вариант: _____

Использование

□ попытки вовлечь меня в преступную или антиобщественную деятельность
□ вербовка в антисоциальные группы, религиозные секты
□ обманное использование моего труда
□ провокация моей активности в социальных сетях (например, чтобы я поставил лайк, сделал репост, пригласил друга)
□ навязывание партнерских программ
□ свой вариант: _____

г. Конкретизируйте, пожалуйста, ущерб, нанесенный этими инцидентами (нужное подчеркните)

□ финансовый
☹ потеря денег
☹ затраты на восстановление здоровья или технического состояния устройств
☹ приобретение кредитных обязательств

☹ свой вариант: _____
□ организационный
☹ нарушение или изменение графика работы
☹ нарушение ритма производственной деятельности
☹ потеря бизнес-проекта
☹ свой вариант: _____
□ психический
☹ потеря сна
☹ ощущение беспокойства, тревоги
☹ появление озлобленности
☹ чувство беспомощности, растерянность
☹ свой вариант: _____
□ технический
☹ отключения и сбои в работе персональных устройств
☹ потеря или искажение информации
☹ выход из строя оборудования
☹ свой вариант: _____
□ социальный
☹ проблемы на работе
☹ проблемы в ближайшем окружении
☹ сложности при коммуникации с другими людьми
☹ свой вариант: _____

д. Сумма нанесенного ущерба и дополнительных затрат, по Вашему мнению, (в денежном эквиваленте) составила

□ до тысячи рублей
□ от 1 до 10 тыс. руб.
□ свыше 10 тыс.
□ ничего

е. Какие меры Вы предпринимали во избежание ущерба от указанных инцидентов?

□ обращался в полицию
□ разбирался в ситуации самостоятельно (возвращал контроль над аккаунтом, устанавливал антивирус, менял пароли и т.п.)
□ обращался с жалобами в администрацию интернет-сайтов на неправомерные действия других пользователей
□ игнорировал подозрительные письма, ссылки и просьбы
□ свой вариант: _____

2. Шкала кибервиктимизации Д.В. Жмурова

Представляет собой унифицированный диагностический инструмент, стандартизованное задание, цель которого определить степень кибервиктимности индивида. Для этого необходимо ответить на 38 вопросов. Вопросы условно разделены на 4 субшкалы:

– *провоцирующее поведение* (ПП, 16 вопросов), т.е. оценка меры и степени вклада жертвы в создание ею благоприятных условий для совершения преступления.

– *защитные стратегии* (ЗС, 8 вопросов) – показатель степени эффективности контрмер, которые предпринимает потенциальная жертва, чтобы избежать негативного влияния.

– *цифровая погруженность* (ЦП, 6 вопросов) – вовлеченность индивида в интернет-коммуникации. Чем она выше, тем больше шансы оказаться жертвой киберпреступников. Это финансовая, эмоциональная сопричастность виртуальному

миру, когда значительный объем социальной жизни перенесен в цифровое пространство.

опыт предыдущей кибервиктимизации (ОВ, 8 вопросов) – имелись ли уже случаи превращения в жертву преступления в цифровом пространстве.

Каждый из вопросов предполагает варианта 3 ответа, которые дифференцированы по степени глубины виктимности носителя, начиная от повышенной и заканчивая степенью близкой к нулевой. Тестовые задания представлены в табл.1.

Таблица 1

Шкала кибервиктимизации Д. Жмурова

S шкл.	№ п/п	Вопрос	3 балла	2 балла	1 балл
ЗП	1	Я пользуюсь антивирусными программами	*не использую*	*устанавливаю нелицензионные или бесплатные*	*обязательно и только лицензионные версии*
ПП	2	Были случаи, когда я посещал сайты для «взрослых»	*бывает, посещаю*	*очень редко*	*никогда*
ЦП	3	В интернете я провожу немало времени	*да, это так*	*достаточно, но не много*	*стараюсь минимизировать время своего пребывания в сети*
ОВ	4	В сети я часто попадаю в неприятные ситуации	*до нескольких раз в год*	*за все время могу вспомнить пару эпизодов*	*такого не бывает*
ЗП	5	Я всегда обращаю внимание на состояние протокола подключения к сети	*никогда*	*иногда, если сайт вызывает подозрения*	*стараюсь всегда проверять безопасность протокола и сертификаты сайта*
ПП	6	По опыту знаю, что многим людям приходится скачивать пиратские программы, видео и аудиоконтент	*это делают все, и я тоже*	*стараюсь этого не делать, хотя иногда приходится*	*пользуюсь только лицензионным ПО*
ЦП	7	Как правило, у меня действующие профили в 2-3 социальных сетях	*да, именно так*	*нет, я присутствую только в одной социальной сети*	*меня нет в социальных сетях*
ОВ	8	Были инциденты, когда меня преследовали в сети	*да, со мной случалось подобное*	*возможно, некоторые люди и проявляли навязчивость*	*нет, меня никто не преследовал*
ЗП	9	На важных аккаунтах я устанавливаю двойную аутентификацию	*в этом нет необходимости*	*да, кое-где я использовал эту системы защиты*	*использую ее почти на всех аккаунтах*
ПП	10	Иногда я устанавливаю на компьютер программы с низким рейтингом и плохими отзывами	*ни вижу в этом ничего плохого*	*да, иногда приходится*	*никогда этого не делаю*
ЦП	11	Я делаю покупки через Интернет	*совершаю на регулярной основе*	*делаю, но только на проверенных сайтах*	*предпочитаю покупать традиционными способами*

Продолжение табл. 1

S шкл.	№ п/п	Вопрос	3 балла	2 балла	1 балл
ОВ	12	Я могу припомнить случаи, когда у меня в интернете украли деньги	*да, у меня пропадали деньги*	*пытались украсть, но ничего не вышло*	*таких происшествий не было*
ЗП	13	Для безопасности я использую VPN и шифрование траффика	*нет, не применяю*	*редко, в случае необходимости*	*постоянно*
ПП	14	Если меня оскорбят на форуме я не буду молчать и отвечу тем же	*да, это справедливо*	*в редких случаях, если буду сильно волноваться*	*почти никогда*
ЦП	15	Все события личной жизни я стараюсь отражать в социальных сетях (фото, посты, прямые эфиры)	*стараюсь делать это регулярно*	*несколько раз в месяц*	*почти не занимаюсь таким*
ОВ	16	Мои личные данные использовались злоумышленниками	*к сожалению, я попадал в такую ситуацию*	*был риск, что моими данными воспользуются, хотя до этого не дошло*	*нет, мои данные надежно защищены*
ЗП	17	Стараюсь своевременно обновлять установленные у меня программы	*не слежу за обновлениями*	*иногда обновляю*	*делаю это систематически*
ПП	18	Временами я читаю письма от незнакомых людей и перехожу по ссылкам, указанным в почте	*конечно читаю, не все люди мошенники*	*бывает, но достаточно редко*	*никогда, сразу удаляю такие письма*
ЦП	19	Онлайн игры для меня важны и интересны	*я весьма увлечен ими*	*периодически играю, но не являюсь фанатом*	*особого интереса нет*
ОВ	20	По телефону мне приходят рассылки (спам) на которые я не давал согласия	*очень часто*	*бывает, но не часто*	*практически не приходят*
ЗП	21	Я не храню персональные и платежные данные в компьютере	*храню в браузере или отдельном файле (черновике почты)*	*храню, т.к. они записываются сами, но стараюсь своевременно чистить*	*сразу удаляю из памяти компьютера*
ПП	22	Я общаюсь с людьми в сетях, хотя понимаю, что в жизни они могут быть не теми, за кого себя выдают	*да, а как иначе?*	*порой встречаются и такие «знакомые»*	*предпочту с такими не контактировать*
ЦП	23	При размещении постов я нередко использую геометки	*почти всегда*	*достаточно редко*	*не использую*
ОВ	24	Порой, для получения информации, приходится игнорировать предупреждения о небезопасности сайта	*да, такое иногда происходит*	*в исключительных случаях*	*на подозрительные сайты не перехожу*

Продолжение табл. 1

S шкл.	№ п/п	Вопрос	3 балла	2 балла	1 балл
ЗП	25	В сети стараюсь пользоваться только платными подписками (кинотеатры, музыка, развлечения)	*нет, ведь есть много бесплатного контента*	*использую официальные сервисы, где можно попользоваться бесплатным периодом*	*да, на постоянной основе*
ПП	26	Иногда я завожу интимные знакомства (романтические отношения) в сети	*считаю, что это естественно и нормально*	*стараюсь этого не делать, хотя и отказываться не стану*	*категорически против*
ОВ	27	Иногда я помогал незнакомцам в интернете (отправлял деньги на благотворительность, выручал материально)	*да, считаю это достойным поведением*	*жертвовал, но только в официальные благотворительные фонды*	*никогда таким не занимался*
ЗП	28	Насколько это возможно, делаю так, чтобы мои социальные сети были приватными	*нет, мой аккаунт открыт и заполнен разнообразной информацией обо мне*	*мой аккаунт закрыт от тех, кто на меня не подписан*	*мои социальные сети закрыты от тех, кого я лично не знаю*
ПП	29	Мне не составляет особого труда вступать в переписку с незнакомыми людьми	*никаких проблем*	*я могу долго сомневаться, но потом все же написать*	*не буду этого делать*
ОВ	30	Для скачивания (доступа) на некоторых сайтах требуется подтверждать свой номер телефона	*приходится часто это делать*	*отношусь к таким сайтам с недоверием, хотя несколько раз вынужден был подтверждать*	*лучше поищу другой сайт, где не нужно этого делать*
ПП	31	Даже, если мой компьютер взломают, ценного там мало	*да, это факт*	*может что-то и найдут*	*там много информации, которую можно использовать в плохих целях*
ПП	32	Покупая что-то в сети, я не всегда проверяю продавца	*да, обычно не проверяю*	*в исключительных случаях, когда думаю, что имею дело с мошенником*	*всегда читаю отзывы, смотрю на площадку размещения и длительность его работы*
ПП	33	Наверное, я соглашусь выполнить опасную работу в интернете, если за нее хорошо заплатят	*почему бы и нет*	*после тщательного обдумывания, не исключаю, что соглашусь*	*вряд ли возьмусь за такое*
ПП	34	Не вижу ничего плохого в заработке на хайп-проектах	*да, можно быстро заработать*	*можно, но должны быть веские аргументы, четкий план и гарантии*	*отношусь к такому отрицательно*
ПП	35	Я использую сайты знакомств, чтобы найти интересных людей	*часто*	*иногда*	*предпочитаю другие формы общения*

Окончание табл. 1

S шкл.	№ п/п	Вопрос	3 балла	2 балла	1 балл
ПП	36	Бывает, я принимаю участие в интернет-лотереях и розыгрышах призов	*да, участвую на регулярной основе*	*участвую только в тех, которые считаю проверенными*	*нет, не участвую*
ПП	37	У меня есть опыт участия в азартных играх онлайн	*да, имеется*	*несколько раз пробовал, но без увлечения*	*нет, не интересно*
ПП	38	Нередко я прохожу различные интернет-опросы	*да, участвую постоянно*	*участвую только в тех, которые считаю проверенными*	*нет, не участвую*

Результаты стандартизации «шкалы кибервиктимизации» представлены в табл. 2.

Таблица 2

Стандартизация шкалы кибервиктимизации Д. Жмурова

Станайн	Число баллов	Характеристика результата
1	0–38	степень кибервиктимности близкая к нулевой или незначительная
2	39–76	средняя степень кибервиктимности
3	77–114	повышенная степень кибервиктимности

Представленные методы отнюдь не являются исчерпывающими. Отдельную область применения представляют собой методики автоматической идентификации кибержертв, а также «виктимологический эксперимент», как образец активного исследовательского инструментария [3]. Он может заключаться в искусственном моделировании виктимогенных условий и эмуляции киберпреступления. Речь о создании своего рода «песочницы» для потенциальных жертв, позволяющей без реальных последствий пережить опыт цифровой дискриминации, чтобы быть готовым в повседневной жизни к подобным событиям.

Сегодня многие исследователи предлагают собственные варианты оценки кибервиктимности. Среди наиболее интересных разработок, посвященных этой проблеме нельзя не упомянуть опросники Ballard & Welch [4]; Balarkrishnan [5]; Games-Guadix et al. [6]; Livozovic & Ham [7]; Powell & Henry [8]; Reyns & Fissel [9]. Отдельные инструменты оценки кибервиктимного потенциала уже апробированы, по сути, являются готовыми и самостоятельными средствами диагностики. К таковым, например, можно отнести, шкалу киберзапугивания Hinduja & Patchin [10]; шкалу кибервиктимизации Garaigordobil [11]; шкалу опыта кибервиктимизации и поведения, связанного с киберзапугиванием R. Lucy et al. [12]; опросник киберагрессии для подростков (CYBA) Álvarez-García et al. [13], шкалу кибержертв и издевательств B. Çetin et al. [14]; шкалу кибер-виктимизации CYBVICS S. Buelga et al. [15] и многие другие. Особое внимание к этим проблемам со стороны ученых из разных стран подчеркивает актуальность методологического обеспечения цифровой виктимологии, а также растущие запросы на отечественные разработки в этой области.

Список использованной литературы

1. Бастрыкин А.И. Преступления против несовершеннолетних в интернет-пространстве: к вопросу о виктимологической профилактике и уголовно-правовой оценке / А.И. Бастрыкин. — DOI 10.17150/2500-4255.2017.11(1).5-12 // Всероссийский криминологический журнал. — 2017. — Т. 11, № 1. — С. 5–12.

2. Воронин Ю.А. Виктимная безопасность: терминологическая интерпретация / Ю.А. Воронин, А.В. Майоров // Всероссийский криминологический журнал. — 2014. — № 1. — С. 43–48.

3. Будякова Т.П. Активные методы в виктимологии / Т.П. Будякова // Всероссийский криминологический журнал. — 2011. — № 3. — С. 42–49.

4. Ballard M.E. Virtual warfare: Cyberbullying and cyber-victimization in MMOG play / M.E. Ballard, K.M. Welch. — DOI 10.1177/155541215592473 // Games and Culture. — 2017. — Vol. 12, iss. 5. — P. 666–491.

5. Balakrishnan V. Cyberbullying among young adults in Malaysia: The roles of gender, age and internet frequency / V. Balakrishnan // Computers in Human Behavior. — 2015. — Vol. 46. — P. 149–157.

6. Prevalence and association of sexting and online sexual victimization among Spanish adults / M. Gamez-Guadix, C. Almendros, E. Borrajo, E. Calvete. — DOI 10.1007/s13178-015-0186-9 // Sexuality Research and Social Policy. — 2015. — Vol. 21. — P. 145–154.

7. Livazovic G. Cyberbullying and emotional distress in adolescents: The importance of family, peers and school / G. Livazovic, E. Ham. — DOI 10.1016/j.heliyon.2019.e01992 // Heliyon. — 2019. —Vol. 5, no. 6. — P. 1–9.

8. Powell A. Technology-facilitated sexual violence victimization: Results from an online survey of Australian adults / A. Powell, N. Henry. — DOI 10.1177/0886260516672055 // Journal of Interpersonal Violence. — 2016. — Vol. 34, iss. 17. — P. 3637–3665.

9. Reyns B.W. Recurring online victimization among college women: Risk factors from within the hookup culture / B.W. Reyns, E.R. Fissel. — DOI 10.1891/0886-6708.VV-D-18-00186 // Violence and Victims. — 2019. — Vol. 34, iss. 4. — P. 701–716.

10. Hinduja S. Social influences on cyberbullying behaviors among middle and high school students / S. Hinduja, J.W. Patchin. — DOI 10.1007/s10964-012-9902-4 // Journal of Youth and Adolescence. — 2013. — No. 42. — P. 711–722.

11. 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. 32, iss. 23. — P. 3556–3576.

12. Betts L.R. Developing the Cyber Victimization Experiences and Cyberbullying Behaviors Scales / L.R. Betts, K.A. Spenser. — DOI 10.1080/00221325.2017.1295222 // The Journal of Genetic Psychology. — 2017. — Vol. 178, iss. 3. — P. 147–164.

13. Validity and reliability of the Cyber-aggression Questionnaire for Adolescents (CYBA) / D. Álvarez-García, A. Barreiro, J. Núcez, A. Dobarro. — DOI 10.1016/j.ejpal.2016.02.003 // The European Journal of Psychology Applied to Legal Context. — 2016. — Vol. 8, no. 2. — P. 69–77.

14. Çetin B. Cyber victim and bullying scale: a study of validity and reliability / B. Çetin, E. Yaman, A. Peker // Computers & Education. — 2011. — Vol. 57, iss. 4. — P. 2261–2271.

15. Psychometric Properties of the CYBVICS Cyber-Victimization Scale and Its Relationship with Psychosocial Variables / S. Buelga, B. Martнnez-Ferrer, M-J. Cava, J. Ortega-Baryn. — DOI 10.3390/socsci8010013 // Social Sciences. — 2019. — Vol. 8, no. 13. — P. 1–13.

References

1. Bastrykin A.I. Online crimes against minors: to the issue of victimological prevention and criminal law assessment. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2017, vol. 11, no. 1, pp. 5–12. (In Russian). DOI: 10.17150/2500-4255.2017.11(1).5-12.

2. Voronin Yu.A., Maiorov A.V. Victimological security: terminological explanation. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2014, no. 1, pp. 43–48. (In Russian).

3. Budyakova T.P. Active methods in victimology. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2011, no. 3, pp. 42–49. (In Russian).

4. Ballard M.E., Welch K.M. Virtual warfare: Cyberbullying and cyber-victimization in MMOG play. *Games and Culture*, 2017, vol. 12, iss. 5, pp. 666–491. DOI:10.1177/155541215592473.

5. Balakrishnan V. Cyberbullying among young adults in Malaysia: The roles of gender, age and internet frequency. *Computers in Human Behavior*, 2015, vol. 46, pp. 149–157.

6. Gamez-Guadix M., Almendros C., Borrajo E., Calvete E. Prevalence and association of sexting and online sexual victimization among Spanish adults. *Sexuality Research and Social Policy*, 2015, vol. 21, pp. 145–154. DOI: 10.1007/s13178-015-0186-9.

7. Livazovic G., Ham E. Cyberbullying and emotional distress in adolescents: The importance of family, peers and school. *Heliyon*, 2019, vol. 5, no. 6, pp. 1–9. DOI: 10.1016/j.heliyon.2019.e01992.

8. Powell A., Henry N. Technology-facilitated sexual violence victimization: Results from an online survey of Australian adults. *Journal of Interpersonal Violence*, 2016, vol. 34, iss. 17, pp. 3637–3665. DOI: 10.1177/0886260516672055.

9. Reyns B.W., Fissel E.R. Recurring online victimization among college women: Risk factors from within the hookup culture. *Violence and Victims*, 2019, vol. 34, iss. 4, pp. 701–716. DOI: 10.1891/0886-6708.VV-D-18-00186.

10. Hinduja S., Patchin J.W. Social influences on cyberbullying behaviors among middle and high school students. *Journal of Youth and Adolescence*, 2013, no. 42, pp. 711–722. DOI: 10.1007/s10964-012-9902-4.

11. Garaigordobil M. Psychometric Properties of the Cyberbullying Test, a Screening Instrument to Measure Cybervictimization, Cyberaggression, and Cyberobservation. Journal of interpersonal violence, 2015, vol. 32, iss. 23, pp. 3556–3576. DOI: 10.1177/0886260515600165.

12. Betts L.R., Spenser K.A. Developing the Cyber Victimization Experiences and Cyberbullying Behaviors Scales. *The Journal of Genetic Psychology*, 2017, vol. 178, iss. 3, pp. 147–164. DOI: 10.1080/00221325.2017.1295222.

13. Álvarez-García D., Barreiro A., Núcez J., Dobarro A. Validity and reliability of the Cyber-aggression Questionnaire for Adolescents (CYBA). *The European Journal of Psychology Applied to Legal Context*, 2016, vol. 8, no. 2, pp. 69–77. DOI: 10.1016/j.ejpal.2016.02.003.

14. Çetin B., Yaman E., Peker A. Cyber victim and bullying scale: a study of validity and reliability. *Computers & Education*, 2011, vol. 57, iss. 4, pp. 2261–2271.

15. Buelga S., Martнnez-Ferrer B., Cava M-J., Ortega-Baryn J. Psychometric Properties of the CYBVICS Cyber-Victimization Scale and Its Relationship with Psychosocial Variables. *Social Sciences*, 2019, vol. 8, no. 13, pp. 1–13. DOI: 10.3390/socsci8010013.

Информация об авторе

Жмуров Дмитрий Витальевич — кандидат юридических наук, доцент, кафедра уголовного права и криминологии, Институт юстиции, Байкальский государственный университет, Иркутск, Российская Федерация, zdevraz@ya.ru, https://orcid.org/0000-0003-0493-265X, SPIN-код: 3644-6102, ResearcherID: ABH-8471-2020.

Author

Dmitriy V. Zhmurov — PhD in Law, Associate Professor, Department of Criminal Law and Criminology, Institute of Justice, Baikal State University, Irkutsk, Russian Federation, zdevraz@ya.ru, https://orcid.org/0000-0003-0493-265X, SPIN-код: 3644-6102, ResearcherID: ABH-8471-2020.

Для цитирования

Жмуров Д.В. Кибервиктимология. Методы и метрика / Д.В. Жмуров. — DOI 10.17150/2411-6262.2022.13(1).29. — EDN ROGYBP // Baikal Research Journal. — 2022. — Т. 13, № 1.

For Citation

Zhmurov D.V. Cybervictimology. Methods and Metrics. *Baikal Research Journal*, 2022, vol. 13, no. 1. (In Russian). EDN: ROGYBP. DOI: 10.17150/2411-6262.2022.13(1).29.