МЕЖДУНАРОДНЫЕ И КОНСТИТУЦИОННЫЕ ОСНОВЫ УГОЛОВНОЙ ЮСТИЦИИ
INTERNATIONAL AND CONSTITUTIONAL BASIS OF CRIMINAL JUSTICE

Научная статья
УДК 343.988
EDN RABUNM
DOI 10.17150/2411-6122.2023.1.5-13

Кибервиктимизация: оценка последствий

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

Аннотация. Настоящая статья посвящена рассмотрению вопроса, касающегося последствий кибервиктимизации, т.е. превращения лица в жертву преступления в виртуальном пространстве. Предложено определение ряда терминов, в частности, «последствия кибервиктимизации», «ущерб от кибервиктимизации», выявлены их сущностные различия. Кроме того, подробно описаны признаки ущерба от кибервиктимизации среди которых выделены: регрессивность, амбивалентность, иррадиированность, полиморфность, ситуационность и диспропорциональность. Предложена авторская типология форм ущерба, основанная, как на одномерной, так и многомерной модели анализа наступивших последствий. Подробно описаны тринадцать основных форм издержек, наступающих в качестве возможного результата виктимизации субъекта цифровой сферы. На основании предложенной классификации, а также фиксации степени нанесенного ущерба автором составлен примерный оценочный лист степени виктимизации в интернете.

Ключевые слова: кибервиктимизация, жертвы в интернете, кибервиктимность, кибервиктимология, интернет-потерпевший, жертвы цифровых преступлений, кибержертва, личность потерпевшего в виртуальном пространстве.

Для цитирования: Жмуров Д.В. Кибервиктимизация: оценка последствий / Д.В. Жмуров. — DOI 10.17150/2411-6122.2023.1.5-13. — EDN RABUNM // Сибирские уголовно-процессуальные и криминалистические чтения. — 2023. — № 1. — С. 5–13.

Original article

Cybervictimization: An Assessment of Consequences

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

Abstract. The author analyses the consequences of cybervictimization, i.e. the situation when a person becomes a victim in virtual space. A number of terms are defined, specifically, “the consequences of cybervictimization”, “the damage inflicted by cybervictimization”, their essential differences are pointed out. Besides, the characteristics of the damage inflicted by cybervictimization are described in detail, including: regressivity, ambivalence, irradiation, polymorphism, situational character and disproportionality. A typology of the forms of damage is proposed, which is based on both one-dimensional and poli-dimensional models of analyzing consequences. A detailed description is provided for thirty main forms of harm that could result from the victimization of a person online. Based on the suggested classification, as well as the recording of the degree of the inflicted damage, the author compiles a sample list for evaluating the degree of victimization on the Internet.

ISSN 2411-6122

Keywords: cybervictimization, victims on the Internet, cybervictimity, cybervictimology, Internet victim, victims of digital crimes, cybervictim, personality of a victim in virtual space.

For citation: Zhmurov D.V. Cybervictimization: An Assessment of Consequences. *Sibirskie Ugolovno-Processual'nye i Kriminalisticheskie Chteniya = Siberian Criminal Procedure and Criminalistic Readings,* 2023, no 1, pp. 5–13. (In Russian). EDN: RABUNM. DOI: 10.17150/2411-6122.2023.1.5-13.

Последствия кибервиктимизации на сегодняшний день недооценены. Не секрет, что наносимый при этом экономический ущерб сопоставим с бюджетами крупных государств, а потери иного характера — вовсе не учитываются. По оценкам экспертных сообществ, ущерб мировой экономике от киберпреступности ежегодно увеличивается и в 2025 г. достигнет суммы в 10,5 трлн дол. в год[1]. При этом еще в 2013 г. он составлял немногим более 113 млрд дол. [1].

Вероятно, не следует отождествлять понятия «последствие кибервиктимизации» и «вред от кибервиктимизации», поскольку они несут разную смысловую нагрузку. Когда речь идет о последствиях, то имеются ввиду негативные и позитивные результаты произошедшего события. А под вредом понимают исключительно неблагоприятное воздействие [2].

Другими словами, вред — это одно из возможных последствий кибервиктимизации, но далеко не единственное. Если для экономической оценки вреда существуют примерные ориентиры и методы, то посчитать психологические, физиологические и моральные издержки — задача чрезвычайно трудная. А положительные эффекты кибервиктимизации (если таковые имеются) ученые вовсе не рассматривают.

В настоящее время формируется научная основа для выработки мер реагирования на криминальные угрозы в сфере высоких технологий [3]. В этом контексте назревает вопрос оценки последствий кибервиктимизации. Это объясняется растущей приверженностью населения Земли к мобильным устройствам (67 % или 5,22 млрд чел. пользуются сотовыми телефонами [4]), ростом цифровой экономики (уже более 2 млрд компаний представлены в мировой сети[2]), проникновением интернета в жизнь большинства представителей человеческой популяции (на начало 2022 г. 60 % или 4,66 млрд чел. являются пользователями глобальной сети [там же]). Очевидно, что все перечисленные макрогруппы являются потенциальными жертвами, ежедневно вносящими свой вклад в совокупный урон от киберпреступности.

При этом нельзя не отметить некоторые сложности, возникающие при подсчете последствий кибервиктимизации. Дело в том, что показатели, принятые для выражения данной категории ущерба, трудно формализуемы и не сводятся к единой системе значений. Это в свою очередь приводит к трудностям группировки этих данных в единый массив, подходящий для математического анализа. Немало форм ущерба плохо адаптируются под «точные», «математические» методы анализа. Как, например, подсчитать вред

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

2 Типологическое исследование «Криминальные денежные потоки в сети Интернет: методы, тенденции и взаимодействие между всеми основными участниками». URL: https://clck.ru/wV2AW (дата обращения: 31.08.2022).

от развития депрессивных состояний у подростка после кибербуллинга? Или оценить влияние этой патологии на дальнейшую жизнь человека?[3]. При этом серьезные методологические затруднения наблюдаются с единой международной методикой расчета вреда, причиненного киберпреступниками [2].

Итак, «*последствие кибервиктимизации*» предлагается понимать как *результат противоправного воздействия на субъекта виртуальной коммуникации*. Эти изменения могут происходить в различных сферах начиная от психологической (трансформация самосознания) и заканчивая организационной (снижение качества менеджмента предприятия). По характеру последствий, ситуация может быть описана как эустресс (оказывающая позитивное влияние на благополучие субъекта) или дистресс (отрицательно или разрушительно влияющая на него). Таким образом, можно предположить о существовании *позитивных* и *негативных* последствий кибервиктимизации.

К *первой* группе относятся: повышение стрессоустойчивости, приобретение навыков противодействия правонарушителям, развитие рефлексии и внимательного отношения к своему поведению, обучение планированию последствий собственной деятельности, развитие навыков коммуникативной гибкости и умения противостоять в ситуации конфликта; приобретение негативного опыта, который в будущем будет использован для преодоления жизненных трудностей и т.п.

Во *вторую* группу включены: снижение функциональности и личной эффективности вплоть до полного прекращения жизнедеятельности; падение показателей адаптации; возникновение отклонений от принятых норм (психологических, поведенческих, социальных, экономических и т.п.); различные формы ущерба и вреда, причиненные субъекту; возникновение негативных состояний депривации и фрустрации; ревиктимизация и опосредованная виктимизация третьих лиц; системные издержки, которые оплачивает общество и проч.

Сосредоточим свое внимание на описании вреда от кибервиктимизации, особенностях его возникновения и типологизации.

Термины «вред» и «ущерб» в рамках настоящего исследования будут пониматься как тождественные. Таким образом, *вред от кибервиктимизации — это* ***нежелательные или неблагоприятные последствия, наступающие для пострадавшего субъекта виртуальной коммуникации***.

Укажем некоторые признаки изучаемого вреда:

Регрессивность предполагает переход от более благоприятного состояния субъекта к менее благоприятному. Выражается в потерях, расходах, невыгодных последствиях, убытках, непредвиденных тратах, физических и моральных страданиях, ухудшении ключевых показателей самочувствия и здоровья.

Амбивалентность означает виртуально-реальный характер причиняемого вреда. Исходным условием выступает его цифровая заданность, возникновение предпосылок реализации исключительно в рамках дигитального пространства, а в качестве результата — выходящий за эти границы материальный характер наступающих последствий (изъятие ценностей, остановка производств, угроза здоровью

3 Cybervictimization, Depression, and Adolescent Internet Addiction: The Moderating Effect of Prosocial Peer Affiliation // Front. Psychol. 2020. 29 Sept. URL: https://doi.org/10.3389/fpsyg.2020.572486.

ISSN 2411-6122

человека). То есть смоделированные в цифровом мире состояния и взаимодействия влекут негативные результаты в объективной реальности.

Иррадиированность выражается в дополнительном негативном воздействии на третьих лиц не принимающих ролевого участия в диаде «жертва — преступник». Можно обозначить некоторые смысловые пересечения с «уровнями виктимизации» Л.В. Франка или термином «рикошетная жертва». Дело в том, что негативные эффекты от киберпреступлений не ограничены сферой личности потерпевшего, почти всегда они выходят за рамки его персоны, отражаются на других участниках социальных отношений. Вред реплицируется (воспроизводится, отражается) на иных акторах, косвенным образом связанных с участником первичной виктимизации. Например, при DDos-атаке могут пострадать не только компания-владелец сайта, но также DNS-провайдер, добросовестные пользователи системы, политические группы и проч. Так, после атаки ботнета Mirai (2016) на сайт провайдера Dyn из-за возросшей нагрузки вместе с Dyn отключился целый ряд популярных площадок (Twitter, PayPal, Netflix и Airbnb) [5]. Или эпизоды с кражами персональной информации, когда с одной стороны вред причиняется частным лицам, а с другой — наносится компаниям, которые не смогли защитить эти данные (вплоть до штрафных санкций). В случаях интернет-мошенничества число потерпевших расширяется подобно «кругам на воде». Естественно, что в первую очередь, страдают физические лица (инвесторы, вкладчики, собственники средств), но во вторую — удар будет нанесен по властям, не способным пресечь такие инциденты или по банку, допустившему незаконное списание, а в конечном итоге — пострадают основы всей цифровой экономики.

Полиморфность — способность сочетать в себе формализуемые и неформализуемые виды убытков. Помимо прямых и косвенных затрат, кибервиктимизация для физических лиц может приводить к ухудшению качества их жизни, экзистенциальным рискам, повышать вероятность девиантного поведения, способствовать появлению соматической симптоматики, осложнению жизненного пути жертвы и проч. Эти особенности ущерба не всегда поддаются точному описанию и расчету.

Ситуационность понимается как зависимость ущерба от значительного количества переменных и факторов. К примеру, оценка материального вреда вследствие атаки на корпоративный сайт, будет зависеть не только от времени простоя ресурса и упущенной выгоды, но также от стоимости работ по ликвидации последствий, которые в каждой стране разные. Так, затраты на восстановление работоспособности оборудования в США или Германии будут стоить больше, чем в России. Психические реакции жертв также варьируются в зависимости от особенностей национального менталитета, определяющего доминирование тех или иных паттернов поведения пострадавшего. Ситуационность вреда может определяться территориальными, этническими, кросс-культурными, экономическими и иными факторами.

Диспропорциональность проявляется в том, что причиненный вред и затраты ресурсов на достижение преступного результата радикальным образом несопоставимы. Как правило, это означает, что серьезных результатов в виртуальной среде можно добиться меньшими усилиями.

Условно можно выделить две основные модели ущерба от кибервик-

тимизации: а) монофакторную и б) мультифакторную. Подобная классификация позволяет избежать дискуссий о типологии вреда и необходимости разнесения его по смежным, иногда пересекающимся между собой и даже спорным категориям.

Однофакторная модель ущерба подразумевает сконцентрированность оценки последствий кибервиктимизации на каком-либо одном ключевом обстоятельстве.

Здесь традиционно рассматриваются разнообразные переменные, начиная от финансовых и заканчивая нематериальными последствиями.

Например, *стоимостной вред* связан с повреждением или изъятием имущества (имущественных благ), имеющих денежное выражение. В данном случае оцениваются реальные потери и ущемление экономических интересов субъекта, угрожающее его функционированию. *Личностный вред* заключается в негативных последствиях для жизни и здоровья человека. А *нематериальный ущерб* предполагает убытки, связанные с наступлением негативных последствий невещественного характера, без соответствующего стоимостного эквивалента.

Однофакторные модели основаны на инструменте анализа, который предполагает мысленное выделение частей изучаемого объекта. Таким образом, к символически обособленным формам ущерба можно отнести:

– *имущественные издержки* (потеря активов; уничтожение или отказ оборудования; утрата денежных средств и их аналогов; неправомерное лишение экономических, политических, личных и иных цифровых прав);

– *информационные издержки* (утрата, повреждение, блокировка, деанонимизация или утечка цифровых активов);

– *энергетические издержки* (лишение доли траффика, электроэнергии и вычислительных мощностей);

– *коммерческие издержки* (снижение производительности труда; перебои в работе с заказчиками; прерывание бизнес-операций; отток потребителей; потеря доли на рынке; снижение стоимости акций; вызванные цифровыми рисками повышение стоимости страхования и рост стоимости капитала на рынках заемных средств; упущенная выгода, иная утрата доходов);

– *институциональные издержки* (расходы на возможные судебные иски; компенсации пострадавшим; затраты, связанные с поиском, сбором доказательств и судебным преследованием нарушителя; расходы на предоставление информации об инциденте клиентам и общественности; оплата штрафов, сопутствующих виктимизации, напр. для юридических лиц — за уплату выкупа вымогателям или небрежность при хранении персональных данных клиентов);

– *акцептные издержки* (оплата лечения и реабилитации, сопряженных с виктимизацией; дальнейшие затраты на обеспечение информационной безопасности; найм новых сотрудников; плата за ремонт и восстановление дискредитированных ресурсов, данных, оборудования; оплата за услуги по раннему противодействию инсайдерской, саботажной и шпионской деятельности);

– *физиологические издержки* (физические затраты, необходимые для преодоления кризисной ситуации; травмы, телесные повреждения, соматические заболевания, патологические состояния организма, смерть). Они могут наступать, например, в результате доведения лица до самоубийства в интернете; неправильного лечения тех или иных заболеваний под влиянием «авторитетных блоггеров»; а также случаев, когда

ISSN 2411-6122

лицо под воздействием интернет-пропаганды отказывается от медицинских услуг или приобретает опасную для здоровья продукцию (БАДы, продовольствие, косметические средства, хозяйственные товары) и проч.;

– *психические издержки* (отрицательные последствия в виде стресса, снижения качества жизни; негативных изменений в поведении; возникновении психических расстройств и сопутствующих им проблем; моральный ущерб в форме нравственных страданий, появление аддикций и проч.);

– *социальные издержки* (выражаются в ухудшении положения личности, как элемента общественного организма, например, через отключение его от трудовой деятельности, распад семьи; иные негативные модификации социального статуса);

– *репутационные издержки* (потеря доверия сотрудников, клиентов, инвесторов; компрометация доброго имени, достоинства и частной репутации, потеря активной аудитории).

Мультифакторная модель *ущерба* представляет подход к его оценке, как к сложному механизму, сочетающему в себе одновременно несколько негативных последствий с выраженным синергетическим эффектом. Оперативной единицей здесь является не какая-то одна переменная (из указанных выше), а их комплекс, разнонаправленно воздействующий на явления объективной действительности. Мультифакторная модель сконфигурирована как набор или общность различных классов ущерба. На взгляд автора, настоящая позиция в наибольшей степени приближена к реальному положению дел.

Представленная модель тяготеет к методу синтеза, основанному на сведении в единое целое всех элементов явления, в нашем случае, ущерба. Можно указать на следующие его виды:

– *структурные или системные издержки*, характеризуются широким и универсальным охватом. Кибервиктимизация по своей природе поликонсеквентна, т.е. влечет несколько разнородных последствий для одного субъекта (из тех, что по отдельности перечислены выше). Например, имущественные издержки у физических лиц, как правило, сочетаются с психическими. Коммерческие потери юридических лиц сопряжены с институциональными, акцептными или репутационными. В этом «коктейле» могут одновременно сосуществовать три и более видов отрицательных или даже положительных последствий, одновременно воздействующих на жертву;

– *средовые издержки* допускающие изменения глобальных условий функционирования субъекта виктимизации и окружающего его мира (макроэкономический, политический, идеологический, экологический, организационный вред, причиненный в результате киберпреступного акта);

– *ожидаемые издержки* акцентируют внимание на комплексном влиянии вредных последствий на дальнейшую судьбу индивида (определяющие качество его будущей жизни, вероятность криминализации и повторной виктимизации) или компании (детерминируют окончание жизненного цикла организации, смену направления основной деятельности).

Безусловно, это не единственная классификация видов ущерба от кибернетических рисков. Европейские исследователи предложили следующий подход к систематизации затрат на киберпреступность и ее негативные последствия. Выделяются прямые потери, косвенные потери и затраты на защиту информации [6].

Кроме того, никто не отменяет традиционно зарекомендовавшие себя классификации вреда на материальный, моральный, социальный, политический и т.д.

Оценка последствий кибервиктимизации может осуществляться и по степени нанесенного ущерба. На первый план здесь выдвигается ухудшение состояния субъекта, которое варьируется в диапазоне от «ничтожного» до «критического». Рассмотрим каждую из степеней тяжести причиняемого вреда:

Ничтожный — не является сколько-нибудь ощутимым для субъекта, может не осознаваться и не приниматься в расчет при планировании дальнейших действий. Для компании является мизерным, таким ущербом можно с легкостью пренебречь.

Незначительный — небольшой по объему, легко устранимый, с минимальными затратами на ликвидацию, существенно не изменяет состояние субъекта, но требует некоторого внимания с его стороны.

Умеренный — ощутимый на уровне не выше среднего, не слишком крупный по размеру и последствиям, но достаточно чувствительный; не влечет крупных затрат и не затрагивает критически важные сферы жизни и функционирования.

Серьезный — опасный, чреватый значительными последствиями, требующими от субъекта адаптационных усилий. На уровне компаний затрудняется выполнение критически важных задач, утрачивается положение на рынке на длительный период (например, до года)[4]. Для физических лиц — характеризуется наступлением тяжких последствий (инвалидность, длительное лечение, психическое заболевание).

Критический — крайне опасный, переломный, связанный с драматическими для жертвы последствиями: прекращением ее функционирования, как самостоятельной единицы или необратимым изменением состояния и качества существования.

Степень вреда, вероятно, должна определятся методом экспертных оценок. Она может рассчитываться по многосторонности охвата виктимизацией разных аспектов жизнедеятельности (финансовой, технической, организационной, психической, социальной). Чем больше этих аспектов вовлечено в поле ущерба, тем он пагубней. Не последнюю роль при этом играют самоотчеты и оценка степени вреда, предложенная самой жертвой, хотя к таким сведениям желательно подходить с некоторой долей осторожности. Итак, эти данные позволяют определить значение и личностный смысл последствий кибервиктимизации. Для формализации ответов целесообразно использовать оценочный лист степени кибервиктимизации. Например, для жертвы — физического лица, он может выглядеть следующим образом (табл.).

Оценка ущерба от кибервиктимизации для экономических субъектов может быть дополнена акцессорными эффектами, которые в основном касаются дополнительных затрат, упущенной выгоды и способности осуществлять экономическую деятельность.

Итак, последствия кибервиктимизации являются глобальной проблемой современного мира. Они затрагивают все сферы человеческой жизни: от экономики до проявлений психической деятельности. При этом являются весьма разнообразными: единичными, когда речь идет об отдельной жертве киберпреступления (интернет-буллинг, мошенничество в сети) или массовыми — в случае кибертеррористических атак. Оценка объемов ущерба, причиненного в результате кибервиктимизации, играет особую роль в понимании реального состояния киберпреступно-

4 Оценка ущерба от нарушения информационной безопасности. URL: https://www.audit-ib.ru/complete-protection/protection-methods/damage-assessment/ (дата обращения: 31.08.2022).

ISSN 2411-6122

Оценочный лист степени виктимизации в интернете

Степень ущерба / *Характер ущерба*	**Ничтожный** Не имеет для меня значения	**Незначительный** Не важно и не особо чувствительно для меня	**Умеренный** Не слишком серьезно по размеру и силе воздействия, хотя и ощутимо	**Серьезный** Опасно для меня, чревато плохими последствиями	**Критический** Крайне тяжело, переломный момент
Финансовый ущерб					
Организационный ущерб					
Психический ущерб					
Технический ущерб					
Социальный ущерб					
	1 б.	2 б.	3 б.	4 б.	5 б.

сти, теоретико-методологической проработке проблемы эффективного комплекса профилактических мер. Оценка последствий кибервиктимизации возможна благодаря использованию разных методов, среди которых: бухгалтерский и экономический анализ, учетно-статистические методы, средства экспертной оценки, индексы вреда преступлений, использующие стандартные сроки тюремного заключения, как обобщающий показатель ущерба и т.п. Вместе с тем, многие эксперты пока убеждены, что подсчет реального ущерба представляет сложную задачу [7; 8]. Что уж говорить про объективное и всестороннее осмысление всех последствий кибервиктимизации.

Список использованной литературы

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

2. Липинский Д.А. Политические причины как современные факторы эволюции компьютерной преступности в Российской Федерации / Д.А. Липинский, К.Н. Евдокимов. — DOI 10.17150/1996-7756.2015.9(1).101-110. — EDN TMGUIT // Криминологический журнал Байкальского государственного университета экономики и права. — 2015. — Т. 9, № 1. — С. 101–110.

3. Ищенко Е.П. Высокие технологии и криминальные вызовы / Е.П. Ищенко, Н.В. Кручинина. — DOI 10.17150/2500-4255.2022.16(2).199-206. — EDN HCUXZN // Всероссийский криминологический журнал. — 2022. — Т. 16, № 2. — С. 199–206.

4. Сергеева Ю. Вся статистика интернета и соцсетей на 2021 год — цифры и тренды в мире и в России / Ю. Сергеева // WebCanape. — 2021. — 02 февр. — URL: https://www.web-canape.ru/business/vsya-statistika-interneta-i-socsetej-na-2021-god-cifry-i-trendy-v-mire-i-v-rossii/ (дата обращения: 31.08.2022).

5. Почекутов С. 8 крупнейших DDoS-атак в истории / С. Почекутов // Timeweb. — 2021. — 22 окт. — URL: https://timeweb.com/ru/community/ articles/samye-gromkie-ddos-ataki-v-istorii (дата обращения: 31.08.2022).

6. Measuring the cost of cybercrime / R. Anderson, C. Barton, R. Bohme [et al.] // Economics of Information Security and Privacy / ed. R. Boohme. — Berlin : Springer, 2013. — P. 265–300.

7. Ляпин А.Е. Киберпреступность как новый объект статистического анализа / А.Е. Ляпин. — EDN ISZLBZ // Статистика и Экономика. — 2021. — № 18 (6). — С. 4–16.

8. Швырев Б.А. Оценка ущерба пользователю от киберпреступности в зарубежных странах / Б.А. Швырев. — EDN VBMVHC // Естественные и технические науки. — 2018. — № 9. — С. 70–72.

References

1. Parhomenko S.V., Evdokimov K.N. Prevention of cybercrime in the Russian Federation: an integrative and comprehensive approaches. *Kriminologicheskii zhurnal Baikal'skogo gosudarstvennogo universiteta ekonomiki i prava = Criminology Journal of Baikal National University of Economics and Law*, 2015, vol. 9, no. 2, pp. 265–276. (In Russian). EDN: TXKVKV. DOI: 10.17150/1996- 7756.2015.9(2).265-276.

2. Lipinsky D.A., Evdokimov K.N. Political reasons as modern factors of the evolution of computer crimes in the Russian Federation. *Criminology Journal of Baikal National University of Economics and Law*, 2015, vol. 9, no. 1, pp. 101–110. (In Russian). EDN: TMGUIT. DOI: 10.17150/1996-7756.2015.9(1).101-110.

3. Ishhenko E.P., Kruchinina N.V. High-tech and criminal challenges. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2022, vol. 16, no. 2, pp. 199–206. (In Russian). EDN: HCUXZN. DOI: 10.17150/2500-4255.2022.16(2).199-206.

4. Sergeeva Ju. All statistics of the Internet and social networks for 2021 — figures and trends in the world and in Russia. *WebCanape*, 2021, February 2. Available at: https://www.web-canape.ru/business/vsya-statistika-interneta-i-socsetej-na-2021-god-cifry-i-trendy-v-mire-i-v-rossii/. (In Russian).

5. Pochekutov S. 8 Biggest DDoS attacks in history. *Timeweb*, 2021, October 22. Available at: https://timeweb.com/ru/community/articles/samye-gromkie-ddos-ataki-v-istorii. (In Russian).

6. Anderson R., Barton C., Bohme R., Clayton R., Eeten M.J.G., Levi M., Moore T., Savage S. Measuring the cost of cybercrime. In R. Boohme (ed.). *Economics of Information Security and Privacy*. Berlin, 2013, pp. 265–300.

7. Lyapin A.E. Cybercrime as a new object of statistical analysis. *Statistika i ekonomika = Statistics and Economics*, 2021, no. 18, pp. 4–16. (In Russian). EDN: ISZLBZ.

8. Shvyrev B.A. Estimation of damage to the user from cybercrime in foreign countries. *Estestvennye i tekhnicheskie nauki = Natural and Technical Sciences*, 2018, no. 9, pp. 70–72. (In Russian). EDN: VBMVHC.

Информация об авторе

Жмуров Дмитрий Витальевич — кандидат юридических наук, доцент, доцент кафедры уголовного права, криминологии и уголовного процесса, Институт юстиции, Байкальский государственный университет, координатор проекта «Национальная энциклопедическая служба России», Байкальский государственный университет, г. Иркутск, Российская Федерация.

Author Information

Zhmurov, Dmitriy V. — Ph.D. in Law, Ass. Professor, Chair of Criminal Law, Criminology and Criminal Process, Institute of Justice, Baikal State University, Coordinator, Project «National Encyclopedic Service of Russia», Irkutsk, the Russian Federation.

Поступила в редакцию / Received 03.10.2022

Одобрена после рецензирования / Approved after reviewing 17.10.2022

Принята к публикации / Accepted 27.01.2023

Дата онлайн-размещения / Available online 23.03.2023