УДК 343.988 **DOI: 10.34670/AR.2023.94.21.092**

Виктимизация населения в глобальных цифровых конфликтах

Жмуров Дмитрий Витальевич

Кандидат юридических наук,
доцент кафедры уголовного права и криминологии,
Байкальский государственный университет экономики и права,
664015, Российская Федерация, Иркутск, ул. Ленина, 11;
e-mail: zdevraz@ya.ru

Аннотация

Статья посвящена вопросам виктимизации населения к ходе глобальных цифровых конфликтов, а именно кибервойн, кибердиверсий или кибертеррористических актов. Автором обоснована актуальность исследования представленной темы, предложены некоторые рабочие определения, в частности термин массовые виктимизирующие действия в сети. Выделены основные типы потерпевших, формирующиеся в ходе указанных событий. Среди них указаны: жертвы дезорганизации, деанонимизации, деклассификации, деморализации, дезинформации и мотивирования. В более общем плане всех пострадавших предложено разделять на две основные группы: избирательных и неизбирательных жертв. Кроме того, на основе анализа зарубежной литературы, приведены описания некоторых особенностей поведения жертв массовой виктимизации в интернете, именованные «эффектом кибертерроризма». В заключении делается вывод о том, что смена парадигмы современных межгосударственных конфликтов требует пересмотра Женевских конвенций и введения в них понятия и правил ведения кибервойны, описания особенностей статуса ее участников.

Для цитирования в научных исследованиях

Жмуров Д.В. Виктимизация населения в глобальных глобальных цифровых конфликтах // Вопросы российского и международного права. 2023. Том 13. № 5А. С. 504-514. DOI: 10.34670/AR.2023.94.21.092

Ключевые слова

Кибервиктимизация, кибервиктимология, кибервиктимность, кибержертва, жертвы в интернете, жертвы кибервойны, потерпевшие от кибертерроризма.

Введение

Виртуальная реальность оказалась не только прибежищем киберпреступности, но и местом военных действий. Она активно осваивается специалистами в области информационной безопасности, кибервойсками, хактивистами и другими игроками. Новый виток противостояния кибернетических сил совпал с проведением специальной военной операции России на Украине. Именно в этот период интенсифицировались кибервойна и кибердиверсионная деятельность. Positive Technologies сообщает, что на виртуальном поле сражения столкнулись более 70 хакерских групп: 46 – проукраинских и 26 – пророссийских. К августу 2022 г. ситуация выровнялась: из 93 группировок на стороне Украины насчитывалось 45, тогда как за Российскую Федерацию выступили 43 объединении.

Основная часть

В сложившихся обстоятельствах весьма перспективным и своевременным представляется изучение виктимологического аспекта происходящих событий, а именно разработка темы жертв крупных виртуальных конфликтов. Несмотря на популярность данной проблематики и ее активное изучение [Кибальник, Волосюк, Иванов, 2021], приходится констатировать, что потерпевшие от кибервойн и кибертерроризма практически никем не рассматриваются. В научной электронной библиотеке E-library не удалось обнаружить ни одной публикации, содержащей в своем наименовании словосочетания «жертва кибертерроризма» или «жертва кибервойны» (по состоянию на 2 ноября 2022 года). Вероятно, причиной этого является то, что эмпирического материала мало, а причиняемый ущерб от указанных действий незначителей. Некоторые авторы высказывают серьезные сомнения во вредоносном потенциале подобных форм борьбы [Галявиева, www…]. Вместе с тем, недооценивать потенциальную опасность обозначенных угроз недальновидно. Нельзя забывать об их относительной новизне [Узденов, 2016], только начавшемся внедрении в практику конфликтов. По мнению автора, кибервойна (кибертерроризм) заключают в себе возможность крупных потерь в будущем, а в цифровом обществе – данные риски возрастают многократно. Это связано с востребованностью информационных методов ведения войн в контексте гибридного противостояния геополитических акторов. Все это станет причиной виктимизации населения, которое является объектом системного воздействия, мишенью деструктивных усилий противоборствующих сторон, подпадая под признаки массовой (групповой) виктимизации. Последняя обнаруживает себя в системном или несистемном множестве актов причинения вреда, объединенных целью истощения противника и нанесения ему инфраструктурного урона.

Следует определить исходные понятия:

– *кибертерроризм* – это осуществление в цифровой среде политически мотивированных актов дестабилизации со стороны неинституциональных субъектов (террористических организаций, квазигосударств);

– *кибердиверсия* – уничтожение и повреждение инфраструктуры противника, осуществляемое посредством воздействия на цифровую среду со стороны институционального субъекта (государства, военного блока);

– *кибервойна* – конфронтация институциональных субъектов в виртуальном пространстве с целью нанесения максимального взаимного ущерба.

Условно эти понятия можно объединить словосочетанием *массовые виктимизирующие*

действия в сети. К их особенностям относятся:

– осуществление по отношению к широкому числу субъектов;
– конечной целью является не столько причинение вреда конкретным лицам, сколько системное разрушение социальных, экономических и цифровых основ общества, а в случае кибертерроризма - провокация страха и запугивание населения [*Sheldon, Hanna, www…*];
– стремление к нанесению физического, организационного и технически необратимого вреда;
– оправдание этих действий какой-либо религиозной, нравственной или политической идеей (доктриной).

Жертв массовых виктимизирующих действий в сети можно разделить на две основные группы: *избирательных* и *неизбирательных*.

Первое, *избирательные жертвы*, т.е. субъекты направленного дискриминирующего воздействия.

Так, после начала специальной военной операции России на Украине, хакерская группа «Anonymous» объявила нашему государству кибервойну. Эксперты констатируют, что атаки носили организованный характер и координировались из США (по сведениям Национального центра кибербезопасности КНР [*Демченко, www…*]). Всего зафиксировано несколько наступательных волн, и они были направлены на заранее известные, персонализированные цели. Первая волна атак была обращена на средства массовой информации (РБК, RT, «Известия», ТАСС). Под вторую попали лидеры мнений (медийные персоны). Третий удар пришелся на структуры, обеспечивающие безопасность и устойчивость социальной системы: МВД, ФСИН, ФАС, ПФ и др.

Таким образом наиболее высокий риск попадания в категорию избирательных жертв имеют [*Jalil, www…*]:

– банковская отрасль, процессинговые центры;
– военные ведомства и компании, связанные с созданием вооружений;
– генерирующие электроэнергию мощности;
– центры управления логистикой, аэрокосмическая отрасль;
– институты коммунального благополучия (системы водоснабжения, энергообеспечения);
– правительственные структуры;
– нефтяные и газовые компании;
– образовательные учреждения: университеты, исследовательские центры;
– торговые и коммерческие структуры;
– хедлайнеры и лидеры общественного мнения (журналисты, политики, блогеры).

Второе, *неизбирательные жертвы* – случайные, заранее неселектируемые пострадавшие. В основном представляют собой граждан одного из государств-участников конфликта, на которых оказывается отрицательное неперсонифицированное воздействие. Это означает, что причинитель вреда при выборе жертв действует хаотически, рассчитывая, что его действия позволят обеспечить максимально широкий охват виктимизируемой аудитории.

Представленная классификация пострадавших не является единственной. К.В. Вишневецкий указывает на существование прямых и косвенных жертв террористических актов, однако эта типология справедлива и для потерпевших от массовых виктимизирующих действий в сети. Под прямыми жертвами понимаются лица непосредственно пострадавшие в результате

инцидента, а косвенными - те, на кого воздействуют вторичные эффекты бедствия [*Вишневецкий, 2013*].

Если расширительно трактовать типологию жертв кибертерроризма В. Д. Корреи, то потерпевших от «массовых виктимизирующих действий» в сети можно разделить на тех, кто столкнулся с *кибер-активными* (cyber-enabled crime) *и кибер-зависимыми* преступными актами (cyber-dependent crime). В первом случае – это потерпевшие от общеуголовных инцидентов, совершаемых в интернете (деяний против конституционных, имущественных и иных прав). Во втором – жертвы специфических компьютерных правонарушений (кражи персональных данных, взлома аккаунта, распространения вредоносных программ и т.д.).

Также В. Д. Корреи предложено понятие «системной жертвы», которая трактуется, как группа взаимосвязанных или смежных устройств, составляющих национальную информационную инфраструктуру и атакованных в политических (военных) целях [*Correia, 2022*]. В контексте близком к понятию «системная жертва» высказывается Ш.А. Джалил, утверждая, что катастрофическая цифровая атака или серия атак, наносят ущерб нации или народу в целом.

В рамках реализации *массовых виктимизирующих действий* основными типами потерпевших могут быть:

1. *Жертвы дезорганизации (дезактивации)*, т.е. нарушения нормального функционирования цифровой и медиа инфраструктуры, затрагивающей неопределённо широкий круг лиц (пострадавшие от internet outage, internet blackout, internet shutdown). Эти понятия связаны с полным или частичным отказом интернет-сервисов от выполнения повседневных функций (информационных, коммуникативных, логистических, коммерческих, инфраструктурных) и причинением пользователям неудобств различной степени выраженности. Как правило, это взломы и DDOS-атаки, направленные на национальные ресурсы: видеохостинги, сайты банков, платежных систем, компоненты электронного правительства, агрегаторы железнодорожных и авиабилетов и др. Подобные акты зачастую не связаны с необратимыми последствиями: они создают временные проблемы, не причиняя катастрофического вреда. Нередко за громкими сообщениями о кибердиверсиях стоят несложные технические манипуляции, которые хоть и мешают работе сайтов, но не приводят к серьёзным последствиям [*Королева, www…*]. Иногда, создается впечатление, что объектами нападения выбираются те, которые было легче скомпрометировать. Известно, например, что проукраинское киберсообщество в качестве целей атак 2022 г. выбрало сайты торговли автозапчастями, магазины бытовой техники, ресурсы локальных органов власти, новостные порталы местного значения и проч. Возможно, нападающие руководствовались принципом «ломай то, что ломается», изначально выбирая несложные и плохо защищенные цели. Однако, нельзя исключать того, что недобросовестные владельцы этих сайтов «списывали» собственные технические проблемы на действия хакеров. Кроме этих «потешных» случаев, не прошли незамеченными глобальные ресурсоёмкие атаки на Сбербанк, платежную систему «Мир», сайт Госуслуг, воплощающие реальное лицо кибервойны.

При этом в качестве сверхзадачи хакерских нападений декларируется переход виртуальных действий в плоскость физического ущерба, создание условий, делающих невозможным быстрое устранение наступающих разрушений. Таким образом, к физическим последствиям атак можно отнести:

– блокирование на продолжительный срок каналов связи и координации, например, во время боевых действий (чрезвычайных ситуаций);

– отключение электроэнергии, которое провоцирует рост вторичных жертв и финансовые потери. Например, в США в результате сбоя энергоснабжения (2003, Нью-Йорк) погибло 90 человек. Моделирование блэкаута в Райнгау-Таунус (Германия) показало, что за первые трое суток произойдет не менее 400 летальных случаев.
– вывод из строя аппаратных средств, способных продуцировать материальные последствия, например использование вируса Win32.Stuxnet для нарушения работоспособности ядерных реакторов;
– попытки провокации человеческих жертв на роботизированных производственных линиях и циклах;
– необратимое уничтожение информации. По мнению ряда экспертов кибермошенничество ушло на второй план, уступив место необратимому шифрованию и удалению информации на серверах с целью причинения непоправимого ущерба;
– снижение возможностей населения на фоне тотальных отказов интернет-инфраструктуры (создание коммуникативного вакуума путем отключения социальных сетей и мессенджеров; уменьшение мобильности благодаря блокированию билетных агрегаторов, сайтов перевозчиков и аэропортов; провокация роста безработицы - для осуществляющих трудовую деятельность удаленно и т.п.).

2. *Жертвы деанонимизации* – пострадавшие от обнародования персональной информации, как элемента глобального киберстолкновения. Зачастую, подобные действия предпринимаются по отношению к широкому кругу лиц, так или иначе связанных с актуальной политической повесткой и текущим конфликтом. Схожие инициативы наблюдались с обеих сторон российско-украинского противостояния. Неоднократно происходили различные вбросы: поименные списки мобилизуемых граждан России; данные агентов Главного управления разведки Министерства обороны Украины и аффилированных с ними лиц; информация о сотрудниках 72-й Центра психологических операций Украины; персональные сведения об участниках запрещенной в России террористической организации «Азов», включая имена и фамилии, номера телефонов, псевдонимы и проч.

3. *Жертвы деклассификации* (*рассекречивания*) – пострадавшие от разглашения важнейшей информации, имеющей стратегическое или тактическое значение и не сводимой к персональным данным. Это материалы, которые государство считается конфиденциальными и подлежащими защите. Это могут быть сведения о военных разработках; документы, касающиеся переговоров с политическими ведомствами других стран; информация о платежном балансе государства; разведывательная и контрразведывательная документация. Разглашение таких сведений является важнейшей частью информационно-цифровой войны и мерой подавления противника. Например, имели место эпизоды с публикацией материалов правительства Украины, согласно которым действия ВСУ координируются разведывательным управлением США; разнарядки на вооружение и военное имущество, поставляемое на Украину государствами НАТО; утечки Центрального банка РФ об аудиторских сделках и владельцах кредитных учреждений; публикация баз электронных писем Министерства культуры РФ, содержащая данные о зарплатах и увольнениях сотрудников, обсуждение дефектов объектов культурного наследия и т.д.

4. *Жертвы деморализации* - лица, морально и психологически дезорганизованные, испытывающие дефицит качеств необходимых для целеполагания и устойчивого социального функционирования (дефекты инициативности, ответственности, дисциплинированности и проч.). Попытки деморализации граждан РФ осуществлялись с украинской стороны, как в

преддверии специальной военной операции на Украине, так и после ее начала. В целях системной дестабилизации общества были задействованы информационные и аналитические подразделения, социальные инженеры, группы влияния в социальных сетях и других медиа, контрпропагандистские команды, псевдопатриотическая агентура, зарубежные СМИ и т.д. Кибероперация под кодовым названием «Смута» запущена в начале 2022 г. Перед пропагандистским аппаратом ВСУ ставилась задача спровоцировать упаднические настроения среди российских граждан, породить сомнения в необходимости военных действий, правильности решений генерального штаба, обострить политическую нестабильность, повысить число акций протестов и неповиновения. Сюжетно в медиапространстве обыгрывался ряд тем, среди которых: якобы скрываемые потери российской армии; низкое качество оружия ВС РФ в зоне СВО; беспредел, происходящий при мобилизации; жизненная необходимость отъезда из страны в текущих условиях; национальные разногласия населения России на фоне СВО (Дагестан, Бурятия, Якутия); плохая работа федеральных и региональных властей; бездействие и безынициативность военного командования и многое другое. Частично за основу были взяты реальные факты и проблемы российского общества, но они были представлены в гипертрофированном виде, доведены до абсурда, интерпретировались некритически с элементами паники и необъективности.

5. *Жертвы дезинформации* – потребители ложной или заведомо искаженной информации, публикуемой одной из конфликтующих сторон намеренно. Целью дезинформации является введение неопределенного числа лиц в заблуждение относительно тех или иных событий. Эти фальсификации могут спровоцировать оппозиционное поведение народных масс или умиротворить их, снизить или повысить уровень поддержки властей внутри страны, тенденциозно расставить акценты на международной арене и т.д. Киберпространство при этом играет немаловажную роль. Так, на англоязычных ресурсах Youtube, Wiki, Facebook, Guardian со времени начала СВО происходит систематическое «очернение» России: информационное поле переполнено смысловыми клише и штампами, такими как «Резня в буче», «Ядерный шантаж Путина», «казни, пытки и ужасное сексуальное насилие российских военнослужащих»..

6. *Жертвы мотивирования* – люди, которых с использованием цифровых технологий, побуждают к криминальной или разрушительной активности в интересах одной из противоборствующих сторон. Речь об активизации агентуры и сочувствующих, провоцировании неустойчивых личностей, курируемых специальными службами, к совершению террористических или диверсионных актов. Такие лица одновременно являются жертвами психологических манипуляций и субъектами преступлений, на которые их склоняют. Так, одним из направлений деятельности украинских секретных служб является мотивирование отдельных граждан России к саботажу, реализации физических угроз и террористическим действиям. Похоже, что случаи «шутинга», публичных вооруженных нападений, техногенных аварий и катастроф в России действительно увеличились после начала проведения СВО. Известно, к примеру, что силы специальных операций Украины проводили вербовку российской молодежи в закрытие сообщества Telegram и VK, с целью вовлечения их в виртуальное минирование – протестную деятельность, связанную с заведомо ложными сообщениями о заложенных бомбах. Применительно к террористическим организациям жертвами мотивирования могут оказаться лица, вовлеченные в соответствующую противозаконную деятельность.

Относительно реакций жертв на кибервоенные действия каких-либо исследований, к сожалению, обнаружить не удалось. В некоторых источниках подобные проблемы

упоминаются, но лишь в контексте изучения жертв кибертерроризма. Основная мысль подобных публикаций сводится к тому, что психологические последствия киберугроз приравниваются к последствиям традиционного терроризма, не исключающим экономическую дестабилизацию, ущерб жизни и здоровью потерпевших, социальный хаос. До настоящего времени указанные последствия носят скорее гипотетический характер. Также было обнаружено, что кибертерроризм на индивидуальном уровне усиливает стресс, беспокойство, фобии, радикализует взгляды и политическую воинственность жертв. Ряд исследователей предложили термин «*эффект кибертерроризма*», который призван описать общую реактологическую модель поведения виктимизированных лиц. Указывается, что для них характерен четкий набор поведенческих ответов, среди которых: психологическое или физическое напряжение, тревога, неуверенность, предпочтение безопасности свободе, переоценка доверия к государственным институтам, поддержка жесткой государственной политики. В виртуальном пространстве эти установки отражают внутреннее принятие мер тоталитарного контроля над Интернетом и призывы к силовому ответу на кибертерроризм (т.н. кинетическое возмездие). Возможно, со временем аналогичным образом будет описан «*эффект кибервойны*», как эмоциональный и поведенческий ответ лиц пострадавших от военных конфликтов, происходящих в цифровой среде.

Заключение

Очевидно, что виктимология кибервойны и кибертерроризма имеет свои особенности. С одной стороны, жертвы этих процессов подвергаются известным формам виктимизации, составляющим суть киберпреступных деяний (фейки, кибербуллинг, киберпреследование, шпионаж, интернет-мошенничества и проч.). С другой – указанные действия подчинены логике противостояния субъектов мировой политики, имеют идеологические и милитаристские корни, значительно выходя за рамки частной криминальной мотивации. Зачастую они направлены на гражданских лиц неизбирательно, как на групповой объект дискриминации. По мнению американских экспертов, такие действия представляют собой нечто большее, чем просто преступления. Перспективы массовой виктимизации населения в Интернете, по мнению автора, реальны, в ограниченных масштабах эти процессы наблюдаются уже сейчас. Смена парадигмы современных межгосударственных конфликтов требует пересмотра Женевских конвенций и введения в них понятия и правил ведения кибервойны, описания особенностей статуса ее участников: комбатантов, некомбатантов, а также мирного населения, страдающего от массовых виктимизирующих действий, осуществляемых в цифровой сфере.

Библиография

1. В Сети рассказали о попытках Украины дестабилизировать ситуацию в России. – URL: https://ria.ru/20220221/ukraina-1774086392.html (дата обращения 01.11.22).
2. *Вишневецкий К. В.* Терроризм. Виктимологический аспект // Теория и практика общественного развития. – 2013. – № 5.– С. 333-340.
3. *Галявиева Л.* Хакеры Killnet осваивают повестку. – URL: https://www.kommersant.ru/doc/5355855 (дата обращения 01.11.22).
4. *Гладков В.* Минцифры пора понять: бывшие кибермошенники давно превратились в террористов – IT-эксперт. – URL: https://www.politnavigator.net/mincifry-pora-ponyat-byvshie-kibermoshenniki-davno-prevratilis-v-terroristov-it-ehkspert.html (дата обращения 02.11.22).
5. *Демченко Н.* Китай сообщил о взломе компьютеров из США для атак на Россию и Украину. – URL: https://www.rbc.ru/technology_and_media/11/03/2022/622ae0a19a7947b70a0319af (дата обращения 29.10.22).

6. *Дремлюга Р. И., Коробеев А. И., Федоров А. В.* Кибертерроризм в Китае: уголовно-правовые и криминологические аспекты // Всероссийский криминологический журнал. – 2017. – № 3 (11). – С. 607-614. – DOI: 10.17150/2500- 4255.2017.11(3).607-614.
7. *Кибальник А. Г., Волосюк П. В., Иванов А. Ю.* Уголовно-правовое противодействие террористическим преступлениям: основные тренды российских диссертационных исследований в 2010–2020 годах // Всероссийский криминологический журнал. – 2021. – № 1 (15). – С. 68–81. – DOI: 10.17150/2500-4255.2021.15(1).68-81
8. Кибер-армия Украины атаковала интернет-сайты Приморья. – URL: https://vestiprim.ru/news/ptrnews/126972-kiber-armija-ukrainy-atakovala-internet-sajty-primorja.html (дата обращения 29.10.22).
9. *Кильдюшкин Р.* Хакер из Killnet анонсировал атаки с человеческими жертвами. – URL: https://www.gazeta.ru/tech/news/2022/08/07/18278294.shtml (дата обращения 02.11.22).
10. *Королева Е.* Противостояние в киберпространстве: хакерское сообщество раскололось после начала спецоперации на Украине. – URL: https://russian.rt.com/world/article/976210-hakery-rossiya-ukraina (дата обращения 29.10.22).
11. *Мельников Д.* Украинские хакеры атаковали уфимское интернет-издание Пруфы.рф. – URL: https://prufy.ru/news/society/130992-ukrainskie_khakery_atakovali_ufimskoe_internet_izdanie_prufy_rf/ (дата обращения 02.11.22).
12. *Мищенко О.* Украинские хакеры атакуют сайт Тюменской областной думы. – URL: https://ura.news/news/1052559643 (дата обращения 02.11.22).
13. *Москаленко В.* Хакеры слили в Сеть новую порцию секретных документов о поставках оружия Киеву. – URL: https://www.politnavigator.net/khakery-slili-v-set-novuyu-porciyu-sekretnykh-dokumentov-o-postavkakh-oruzhiya-kievu.html (дата обращения 01.11.22).
14. Популярнейший в России магазин электроники атакован из Украины? – URL: https://vostokmedia.com/news/2022-08-28/populyarneyshiy-v-rossii-magazin-elektroniki-atakovan-iz-ukrainy-1257392 (дата обращения 29.10.22).
15. Резня в Буче. – URL: https://ru.m.wikipedia.org/wiki/Резня_в_Буче (дата обращения 29.10.22).
16. *Репин А.* «Вербуют молодёжь, обучают в закрытых чатах»: как кибертерроризм в России связан с киевскими силовиками. – URL: https://russian.rt.com/ussr/article/948839-kiber-terrorism-ukraina-minirovanie-kriptovaluta (дата обращения 02.11.22).
17. Российские IT-специалисты успешно отражают хакерские атаки. – URL: https://bel.ru/news/2022-03-23/rossiyskie-it-spetsialisty-uspeshno-otrazhayut-hakerskie-ataki-382363 (дата обращения 29.10.22).
18. Российские IT-специалисты успешно отражают хакерские атаки. – URL: https://bel.ru/news/2022-03-23/rossiyskie-it-spetsialisty-uspeshno-otrazhayut-hakerskie-ataki-382363 (дата обращения 29.10.22).
19. Российские хакеры на сутки лишили украинские власти закрытой связи. – URL: https://ria.ru/20220602/khakery-1792511042.html (дата обращения 02.11.22).
20. *Ростовцев А.* Хакеры перехватили документы разведки США, направлявшиеся Украине. – URL: https: www.politnavigator.net/khakery-perekhvatili-dokumenty-razvedki-ssha-napravlyavshiesya-ukraine.html (дата обращения 01.11.22).
21. *Туронок С. Г.* Информационно-коммуникативная революция и новый спектр военно-политических конфликтов / Полис. Политические исследования. – 2003. – № 1. – С. 24-38.
22. *Узденов Р. М.* Новые границы киберпреступности // Всероссийский криминологический журнал. – 2016. – № 4 (10). – С. 649-655. – DOI: 10.17150/2500-4255.2016.10(4).649-655.
23. Хакер узнал об информационно-психологических операциях Украины в России. – URL: https://ria.ru/20220623/tsentr-1797448543.html (дата обращения 01.11.22).
24. Хакерская атака и утечка данных объемом 700 Гбайт. – URL: https://clck.ru/32YgxF (дата обращения 01.11.22).
25. Хакеры Anonymous слили в сеть данные почти 306 тысяч человек, которых собираются мобилизовать. – URL: https://kun.uz/ru/news/2022/09/22/xakery-anonymous-slili-v-set-dannyye-pochti-306-tysyach-chelovek-kotoryx-sobirayutsya-mobilizovat (дата обращения 01.11.22).
26. Хакеры RaHDIt выложили в открытый доступ данные украинских разведчиков. – URL: https://ria.ru/20220706/razvedka-1800567287.html (дата обращения 01.11.22).
27. Хакеры рассекретили данные о спецоперации Украины на территории России. – URL: https://azned.net/hakery-rassekretili-dannye-o-specoperacii-ukrainy-na-territorii-rossii/ (дата обращения 01.11.22).
28. *Хижняк Н.* Пять способов, которыми хакеры могут убить вас прямо сейчас. – URL: https://hi-news.ru/technology/pyat-sposobov-kotorymi-xakery-mogut-ubit-vas-pryamo-sejchas.html (дата обращения 02.11.22).
29. «Язычник, родновер, ведист, греко-католик»: хакеры опубликовали списки состава националистической группировки «Азов». – URL: https://rusnext.ru/news/1581098228 (дата обращения 01.11.22).
30. Anonymous выложили 28 ГБ информации Центробанка России. Эксперты не увидели в «утечке» ничего секретного. – URL: https://www.ixbt.com/news/2022/03/26/anonymous-vylozhili-28-gb-informacii-centrobanka-

rossii.html (дата обращения 01.11.22).
31. *Correia J. V.* An explorative study into the importance of defining and classifying cyber terrorism in the United Kingdom // SN Computer Science. – 2022. – No. 3. – DOI: 10.1007/s42979-021-00962-5
32. *Gross M. L., Canetti D., Vashdi D. R.* Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes // Journal of Cybersecurity. – 2017. – No. 1 (3). – Pp. 49-58. – DOI: 10.1093/cybsec/tyw018
33. *Gross M. L., Canetti D., Vashdi D. R.* The psychological effects of cyber terrorism // Bulletin of the Atomic Scientists. – 2016. – No 72 (5). – Pp. 284-291. - DOI: 10.1080/00963402.2016.1216502.
34. *Hughes K.* Energy collapse: First blackout simulation in German district predicts 400 deaths in 96 hours. – URL: https://www.naturalnews.com/2022-09-20-german-blackout-simulation-400-deaths-96-hours.html (дата обращения 02.11.22).
35. *Jalil S. A.* Countering cyber terrorism effectively: Are we ready to Rumble? – URL: https://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154 (дата обращения 29.10.22).
36. *Lux L. M.* Una definición de ciberterrorismo // Revista chilena de derecho y tecnología. – 2018. – No. 2 (7). – DOI: 10.5354/0719-2584.2018.51028
37. *Naidu P.* A new list has appeared of pro Ukraine and pro Russian hackers, Reports. – URL: https://www.thetechoutlook.com/news/technology/security/a-new-list-has-appeared-of-pro-ukraine-and-pro-russian-hackers-reports (дата обращения 02.11.22).
38. Putin's nuclear blackmail of Ukraine and the West continues. – URL: https://www.foxnews.com/opinion/putin-nuclear-ukraine-west-judith-miller (дата обращения 29.10.22).
39. *Sheldon R., Hanna K. T.* Cyberterrorism. – URL: https://www.techtarget.com/searchsecurity/definition/cyberterrorism (дата обращения 29.10.22).
40. *Tondo L.* Russia has committed war crimes in Ukraine, say UN investigators. – URL: https://www.theguardian.com/world/2022/sep/23/russia-has-committed-war-crimes-in-ukraine-say-un-investigators (дата обращения 29.10.22).

Victimization of the population in global digital conflicts

Dmitrii V. Zhmurov

PhD in Law,
Associate Professor, Department of Criminal Law and Criminology,
Baikal State University of Economics and Law,
664015, 11, Lenina str., Irkutsk, Russian Federation;
e-mail: zdevraz@ya.ru

Abstract

The article is devoted to the issues of victimization of the population in the course of global digital conflicts, namely cyber wars, cyber sabotage or cyber terrorist acts. The relevance of the study of the presented topic is substantiated, some working definitions, in particular the term "mass victimizing actions" in the network are suggested by author. The main types of victims that are formed in the course of these events are identified. Victims of disorganization, deanonymization, declassification, demoralization, disinformation and motivation are among them. More generally, all victims are proposed to be divided into two main groups: selective and non-selective victims. In addition, based on the analysis of foreign literature, descriptions of some features of the behavior of victims of mass victimization on the Internet, called the «effect of cyberterrorism», are given. In conclusion, it is concluded that a change in the paradigm of modern interstate conflicts requires a revision of the Geneva Conventions and the introduction of the concept and rules of cyber warfare, a description of the features of the status of its participants.

For citation

Zhmurov D.V. (2023) Viktimizatsiya naseleniya v global'nykh global'nykh tsifrovykh konfliktakh [Victimization of the population in global digital conflicts]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 13 (5A), pp. 504-514. DOI: 10.34670/AR.2023.94.21.092

Keywords

Cybervictimization, cybervictimology, cybervictimity, cybervictim, Internet victim, victims on the Internet, victims of cyberwarfare, victims of cyberterrorism

References

1. The Network told about Ukraine's attempts to destabilize the situation in Russia. – URL: https://ria.ru/20220221/ukraina-1774086392.html (accessed 01.11.22).
2. Vishnevetsky K. V. Terrorism. Victimological aspect // Theory and practice of social development. - 2013. – No. 5.– pp. 333-340.
3. Galyavieva L. Killnet hackers master the agenda. – URL: https://www.kommersant.ru/doc/5355855 (accessed 01.11.22).
4. Gladkov V. It's time for the Ministry of Finance to understand: former cybercriminals have long turned into terrorists – IT expert. – URL: https://www.politnavigator.net/mincifry-pora-ponyat-byvshie-kibermoshenniki-davno-prevratilis-v-terroristov-it-ehkspert.html (accessed 02.11.22).
5. Demchenko N. China reported hacking computers from the United States for attacks on Russia and Ukraine. – URL: https://www.rbc.ru/technology_and_media/11/03/2022/622ae0a19a7947b70a0319af (accessed 29.10.22).
6. Dremlyuga R. I., Korobeev A. I., Fedorov A.V. Cyberterrorism in China: criminal law and criminological aspects // All-Russian Journal of Criminology. – 2017. – № 3 (11). – Pp. 607-614. – DOI: 10.17150/2500- 4255.2017.11 (3) .607-614.
7. Kibalnik A. G., Volosyuk P. V., Ivanov A. Yu. Criminal and legal counteraction to terrorist crimes: the main trends of Russian dissertation research in 2010-2020 // All-Russian Criminological Journal. – 2021. – № 1 (15). – Pp. 68-81. – DOI: 10.17150/2500-4255.2021.15(1) .68-81
8. The cyber army of Ukraine attacked the Internet sites of Primorye. – URL: https://vestiprim.ru/news/ptrnews/126972-kiber-armija-ukrainy-atakovala-internet-sajty-primorja.html (accessed 29.10.22).
9. Kildyushkin R. Hacker from Killnet announced attacks with human victims. – URL: https://www.gazeta.ru/tech/news/2022/08/07/18278294.shtml (accessed 02.11.22).
10. Koroleva E. Confrontation in cyberspace: the hacker community split after the start of the special operation in Ukraine. – URL: https://russian.rt.com/world/article/976210-hakery-rossiya-ukraina (accessed 29.10.22).
11. Melnikov D. Ukrainian hackers attacked the Ufa online publication Proofs.rf. – URL: https://prufy.ru/news/society/130992-ukrainskie_khakery_atakovali_ufimskoe_internet_izdanie_prufy_rf / (accessed 02.11.22).
12. Mishchenko O. Ukrainian hackers attack the website of the Tyumen Regional Duma. – URL: https://ura.news/news/1052559643 (accessed 02.11.22).
13. Moskalenko V. Hackers leaked a new batch of secret documents on the supply of weapons to Kiev. – URL: https://www.politnavigator.net/khakery-slili-v-set-novuyu-porciyu-sekretnykh-dokumentov-o-postavkakh-oruzhiya-kievu.html (accessed 01.11.22).
14. The most popular electronics store in Russia was attacked from Ukraine? – URL: https://vostokmedia.com/news/2022-08-28/populyarneyshiy-v-rossii-magazin-elektroniki-atakovan-iz-ukrainy-1257392 (accessed 29.10.22).
15. Massacre in Bucha. – URL: https://ru.m.wikipedia.org/wiki/Reznya_v_buche (accessed 29.10.22).
16. Repin A. "They recruit young people, teach in closed chats": how cyberterrorism in Russia is connected with the Kiev security forces. – URL: https://russian.rt.com/ussr/article/948839-kiber-terrorism-ukraina-minirovanie-kriptovaluta (accessed 02.11.22).
17. Russian IT specialists successfully repel hacker attacks. – URL: https://bel.ru/news/2022-03-23/rossiyskie-it-spetsialisty-uspeshno-otrazhayut-hakerskie-ataki-382363 (accessed 29.10.22).
18. Russian IT specialists successfully repel hacker attacks. – URL: https://bel.ru/news/2022-03-23/rossiyskie-it-spetsialisty-uspeshno-otrazhayut-hakerskie-ataki-382363 (accessed 29.10.22).
19. Russian hackers deprived the Ukrainian authorities of closed communication for a day. – URL: https://ria.ru/20220602/khakery-1792511042.html (accessed 02.11.22).
20. Rostovtsev A. Hackers intercepted US intelligence documents sent to Ukraine. – URL: https: www.politnavigator.net/khakery-perekhvatili-dokumenty-razvedki-ssha-napravlyavshiesya-ukraine.html (accessed

01.11.22).
21. Turonok S. G. Information and communication revolution and a new spectrum of military-political conflicts / Polis. Political studies. - 2003. – No. 1. – pp. 24-38.
22. Uzdenov R. M. New frontiers of cybercrime // All-Russian Criminological Journal. – 2016. – № 4 (10). – Pp. 649-655. – DOI: 10.17150/2500-4255.2016.10(4) .649-655.
23. The hacker learned about the information and psychological operations of Ukraine in Russia. – URL: https://ria.ru/20220623/tsentr-1797448543.html (accessed 01.11.22).
24. Hacker attack and data leak of 700 GB. – URL: https://clck.ru/32YgxF (accessed 01.11.22).
25. Anonymous hackers have leaked the data of almost 306 thousand people to the network, who are going to be mobilized. – URL: https://kun.uz/ru/news/2022/09/22/xakery-anonymous-slili-v-set-dannyye-pochti-306-tysyach-chelovek-kotoryx-sobirayutsya-mobilizovat (accessed 01.11.22).
26. The hackers of RaHDIt have made the data of Ukrainian intelligence officers publicly available. – URL: https://ria.ru/20220706/razvedka-1800567287.html (accessed 01.11.22).
27. Hackers have declassified data on the special operation of Ukraine on the territory of Russia. – URL: https://azned.net/hakery-rassekretili-dannye-o-specoperacii-ukrainy-na-territorii-rossii / (accessed 01.11.22).
28. Khizhnyak N. Five ways hackers can kill you right now. – URL: https://hi-news.ru/technology/pyat-sposobov-kotorymi-xakery-mogut-ubit-vas-pryamo-sejchas.html (accessed 02.11.22).
29. "Pagan, Rodnover, Vedist, Greek Catholic": hackers published lists of the composition of the nationalist group "Azov". – URL: https://rusnext.ru/news/1581098228 (accessed 01.11.22).
30. Anonymous posted 28 GB of information from the Central Bank of Russia. Experts did not see anything secret in the "leak". – URL: https://www.ixbt.com/news/2022/03/26/anonymous-vylozhili-28-gb-informacii-centrobanka-rossii.html (accessed 01.11.22).
31. Correia J. V. An explorative study into the importance of defining and classifying cyber terrorism in the United Kingdom // SN Computer Science. – 2022. – No. 3. – DOI: 10.1007/s42979-021-00962-5
32. Gross M. L., Canetti D., Vashdi D. R. Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes // Journal of Cybersecurity. – 2017. – No. 1 (3). – Pp. 49-58. – DOI: 10.1093/cybsec/tyw018
33. Gross M. L., Canetti D., Vashdi D. R. The psychological effects of cyber terrorism // Bulletin of the Atomic Scientists. – 2016. – No 72 (5). – Pp. 284-291. - DOI: 10.1080/00963402.2016.1216502.
34. Hughes K. Energy collapse: First blackout simulation in German district predicts 400 deaths in 96 hours. – URL: https://www.naturalnews.com/2022-09-20-german-blackout-simulation-400-deaths-96-hours.html (дата обращения 02.11.22).
35. Jalil S. A. Countering cyber terrorism effectively: Are we ready to Rumble? – URL: https://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154 (дата обращения 29.10.22).
36. Lux L. M. Una definición de ciberterrorismo // Revista chilena de derecho y tecnología. – 2018. – No. 2 (7). – DOI: 10.5354/0719-2584.2018.51028
37. Naidu P. A new list has appeared of pro Ukraine and pro Russian hackers, Reports. – URL: https://www.thetechoutlook.com/news/technology/security/a-new-list-has-appeared-of-pro-ukraine-and-pro-russian-hackers-reports (дата обращения 02.11.22).
38. Putin's nuclear blackmail of Ukraine and the West continues. – URL: https://www.foxnews.com/opinion/putin-nuclear-ukraine-west-judith-miller (дата обращения 29.10.22).
39. Sheldon R., Hanna K. T. Cyberterrorism. – URL: https://www.techtarget.com/searchsecurity/definition/cyberterrorism (дата обращения 29.10.22).
40. Tondo L. Russia has committed war crimes in Ukraine, say UN investigators. – URL: https://www.theguardian.com/world/2022/sep/23/russia-has-committed-war-crimes-in-ukraine-say-un-investigators (дата обращения 29.10.22).