УДК 159.923.5

КИБЕРСТАЛКИНГ КАК УГРОЗА ПСИХОЛОГИЧЕСКОМУ БЛАГОПОЛУЧИЮ ЛИЧНОСТИ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ

Батеева А.А.

магистрант первого года обучения,
«Саратовский национальный исследовательский
государственный университет имени Н.Г.Чернышевского»
СГУ имени Н.Г. Чернышевского, г. Саратов, Российская Федерация
anastasiabesschetnova@yandex.ru

Статья посвящена рассмотрению проблемы кибersталкинга как угрозы психологическому благополучию личности в условиях современного цифрового общества, сущность которого проявляется в причинении умышленного, многократного вреда жертве, включая запугивание, угрозы, преследование, осуществляемого в Интернет-пространстве при помощи электронных устройств; дано определение понятий «психологическое благополучие», «виктимизация», «кибервиктимизация», «кибersталкинг»; на основе анализа отечественной и зарубежной литературы выделены виды и ключевые индикаторы кибersталкинга, даны рекомендации по безопасному поведению в сети Интернет.

Ключевые слова: кибersталкинг, Интернет, киберпреступление, виктимизация, кибервиктимизация, жертва.

CYBERSTALKING AS A THREAT TO INDIVIDUAL PSYCHOLOGICAL WELFARE IN THE INTERNET

The article is devoted to the consideration of the problem of cyberstalking as a threat to the psychological well-being of a person in a modern digital society, the essence of which is manifested in causing intentional, repeated harm to the victim, including intimidation, threats, harassment carried out in the Internet space using electronic devices. The definition of the concepts of "psychological well-being", "victimization", "cyber-victimization", "cyber-stalking" is given. Based on the analysis of domestic and foreign literature, the types and key indicators of cyber-stalking are identified, recommendations are given regarding the safe behavior in the Internet.

Keywords: cyber-stalking, Internet, cybercrime, victimization, cyber-victimization, victim.

В настоящее время в науке психологическое благополучие личности как социально-психологический феномен рассматривается с нескольких позиций: во-первых, как позитивное психологическое функционирование личности, включая самопринятие, отношения с окружающими, автономию, управление окружающей средой, цель в жизни, личностный рост (гуманистический подход – представители Д. Биррен, Ш. Бюлер, А. Маслоу, Г. Олпорт, К. Рифф, К. Роджерс, Э. Эриксон, К. Г. Юнг); во-вторых, как удовлетворенность/неудовлетворенность жизнью, возникающая из-за соблюдения/нарушения аффектов позитивного или негативного типа (гедонистический подход – представители Н. Брэдберн, Э. Динер); в-третьих, как способность к самореализации, достижению счастья, полноты бытия (эвдемонистический подход – представители А. Вотермен, А. А. Кроник), отсутствие которого служит основанием

для констатации его антипода – психологического неблагополучия, приводящего к нарушениям процесса адаптации и социализации личности, формированию деструктивных, девиантных форм поведения, в частности, виктимной, аддиктивной и делинквентной активности приспособительного характера, специфических личностных структур или соматических реакций. В результате формируется виктимная личность, характеризующаяся высоким уровнем уязвимости.

Термин «виктимность» введен Л. В. Франком, который обозначает реализованную или потенциальную предрасположенность, способность стать жертвой преступления при определенных обстоятельствах, либо избежать опасности там, где она объективно предотвратима в силу объективных и субъективных обстоятельств [4]. Другими словами, виктимность личности складывается из личностного и ситуационного компонентов, которые взаимосвязаны и взаимозависимы между собой.

Кроме того, выделяют общую виктимность, зависящую от социальных, ролевых, гендерных, возрастных характеристик индивида, и специальную, реализующуюся в установках, свойствах и атрибуциях личности.

По форме проявления виктимность подразделяется на эвентуальную, т.е. случайную, обусловленную причинно-следственным комплексом факторов при определенных условиях стать жертвой преступного посягательства, и децидивную, т.е. способность стать жертвой в результате принятия виктимогенного решения и/или виктимной активности. Случайное виктимное поведение часто обусловлено неосторожностью, доверчивостью, неопытностью, в то время как децидивное спровоцировано активной, настойчивой, требовательной манерой решения проблем.

Д.В. Ривман выделяет следующую типологию жертв: 1) агрессивные жертвы, чье поведение направлено на индивида как источника причинения вреда и часто выражается в оскорблениях, клевете, издевательствах и пр.; 2) активные жертвы, чье поведение не связано с нападением, однако причинение им вреда происходит при их непосредственном участии вследствие подстрекательства, неосторожных действий; 3) инициативные жертвы, причинение вреда которым происходит из-за их инициативных действий по должности или общественному положению; 4) пассивные жертвы составляют группу лиц, не оказывающих сопротивления, противодействия преступнику; 5) некритичные жертвы, неспособные критично оценить реальную или потенциальную угрозу (лица с низким интеллектом, несовершеннолетние, больные) [3].

По мнению исследователей, для индивидов, сознательно избирающих роль жертвы, характерны такие аспекты поведения, как установка на беспомощность, низкая самооценка, ожидание помощи извне, запуганность, иногда конфликтность и агрессия, что, в конечном счете, приводит к вовлечению их в криминогенные кризисные ситуации, как в реальной, так и в виртуальной среде [5,7,10]. В связи с этим, в современной литературе наряду с вышеуказанным понятием «виктимизация» существует термин «кибервиктимизация», т.е. виктимизация личности в Интернет-пространстве.

В современном мире большое распространение получил такой вид кибер-агрессии как киберсталкинг (англ. stalk – «преследовать», «выслеживать»), который представляет собой причинение умышленного и многократного вреда жертве, а также членам ее семьи (преследование, запугивание, террор, рассылка сообщений с угрозами), с помощью электронных устройств (компьютеров, сотовых телефонов и др.) [6].

На основе анализа и систематизации отечественного и зарубежного опыта, в частности, работы Л. Макфарлейна и П. Бокюза «Исследование хищнического поведения в киберпространстве: типологии киберсталкеров» (“An Exploration of Predatory Behaviour in Cyberspace: Toward a Typology of Cyberstalkers”) (пер. автора), можно выстроить следующую классификацию типов киберсталкеров [10]:

Мстительный киберсталкер (vindictive cyberstalker) – действует, движимый желанием возмездия за фактическое или предполагаемое оскорбление или унижение, преследуя свою жертву с конкретным намерением причинить ей страдания, вызвать страх за свою жизнь и безопасность. Данный тип отличается особой жестокостью и в большинстве случаев осуществляет свое намерение в автономном режиме.

Сдержанный киберсталкер (composed cyberstalker) – терроризирует своих жертв с целью причинения им постоянного неудобства, эмоционального напряжения, раздражения, не пытаясь установить с ними прямого контакта.

Интимный киберсталкер (Intimate cyberstalker) – предпринимает настойчивые и неоднократные попытки добиться взаимного чувства и/или привлечь внимание объекта своей страсти, используя электронную почту, веб-дискуссионные группы, электронные сайты знакомств. Данный тип кибersталкера можно условно разделить на две подгруппы: 1) «бывшие близкие», т.е. те, кто активно пытается возобновить общение с человеком, с которым ранее имел близкие отношения или тесное знакомство, несмотря на отсутствие такого желания у оппонента; 2) «влюбленные» – стремятся стремительно развить межличностные отношения, установить тесный контакт с жертвой, не соблюдая при этом социальные правила, регулирующие процесс ухаживания, а в случае получения отказа, начинают активно преследовать жертву.

Коллективные киберсталкеры (collective cyberstalkers) – представляют собой группу из нескольких человек, которые осуществляют травлю с целью сбора информации для дискредитации жертвы при помощи угроз, рассылки спама, взлома почты, кражи личных данных, запугивания мультимедийными файлами.

Кроме того, кибersталкинг можно идентифицировать по следующим ключевым индикаторам [11]: во-первых, выдвижение ложных обвинений, что проявляется в стремлении кибersталкера опорочить репутацию жертвы, размещая заведомо ложную информацию о ней в социальных сетях, блогах, чатах, создавая фиктивные веб-сайты или другие учетные записи от ее имени; во-вторых, сбор информации о жертве, т.е. личных, конфиденциальных данных посредством взаимодействия с друзьями, подписчиками, членами ее семьи, реже прибегая к услугам частного детектива; в-третьих, мониторинг деятельности жертвы в Интернет-пространстве, посредством отслеживания IP-адреса жертвы, взлома учетных записей ее социальных сетей, электронной почты и других аккаунтов; в-четвертых, привлечение других пользователей сети к преследованию жертвы, что выражается в вовлечении широкого круга лиц, часто обманным путем, к травле жертвы; в-пятых, ложная виктимизация, как способ перекладывания вины с преступника на жертву, позволяет кибersталкеру обвинить свою жертву в его преследовании; в-шестых, заказ товаров и/или услуг на имя жертвы для дискредитации ее репутации, является характерным отличием кибersталкинга от других видов виктимизации, когда кибер-преступник заказывает, например интимные товары, на имя жертвы, которые приносят, ей домой или на работу.

Совокупность всех перечисленных индикаторов используется кибersталкерами для усиления давления на жертву путем нагнетания обстановки, усиления чувства страха, тревоги, панических атак, нестабильного эмоционального состояния жертвы преследования. По результатам исследования Р.М. Ковальски, киберзапугивание вызывает более высокий уровень тревоги и депрессии, чем обычное издевательство, что связанно напрямую с анонимностью киберпреступника [9, с. 97].

Ряд исследований, проведенных за рубежом, показывает широкую распространенность и общественную опасность кибersталкинга как социального феномена. Например, по статистическим данным в США 7,5 млн людей ежегодно страдают от навязчивого преследования; в 70 % случаев жертва и преступник живут в разных штатах; 67 % жертв кибersталкинга одиноки, 31 % женаты; 61 % женщин и 44 % мужчин преследуются своими бывшими сожителями; чаще всего от кибертравли

страдают люди в возрасте от 18 до 29 лет; более 30 % кибератак начинаются в социальных сетях, в частности на Facebook, или по электронной почте; 41 % жертв получает письма, сообщения, звонки с нежелательным контентом примерно один раз в неделю [1, с. 179].

Наибольшего распространения феномен кибersталкинга достиг в Великобритании, Канаде, Новой Зеландии, Норвегии, Польше, США, что привело к введению в национальное законодательство статей, предусматривающих уголовную ответственность за реальное или виртуальное преследование граждан. Так, в Канаде уголовная ответственность за преследование была введена еще в 1993 году (статья 264) наряду с такими составами преступления как клевета, причинение вреда, угроза применения насилия и принуждение [6, с. 2]. Примерам уголовно-наказуемых действий в Канаде считаются: любые нежелательные контакты в сети Интернет (чаты, форумы, социальные сети, мессенджеры, электронная почта); беспрерывная рассылка смс- и голосовых сообщений; постоянные звонки и сброс после ответа; выведывание личной информации о человеке у друзей, подписчиков и родственников; нежелательные подарки.

Современным примером может служить введение отдельной статьи в законодательство Норвегии в июле 2016 г., предусматривающей уголовную ответственность за сталкинг (кибersталкинг). По данным Интернет-издания "The Local": «лицо, систематически угрожающее, преследующее, следящее или контактирующее с другим лицом, против воли последнего, может быть подвергнуто наказанию до четырёх лет лишения свободы» [2].

Другими словами, политика ряда зарубежных стран направлена на обеспечение безопасности граждан в сети Интернет, для чего предпринимаются меры по ее защите: мониторинг и анализ современной ситуации; изменения и дополнения в нормативно-правовые акты, информирование граждан о существовании угроз и рисков в Интернет-пространстве. Вместе с тем, в большинстве стран мира, в том числе и в России, отдельные статьи, регламентирующие данное явление, отсутствуют.

Несмотря на это, в российском законодательстве существуют нормативно-правовые акты, предусматривающие проведение комплекса мер, направленных на профилактику и защиту информационной безопасности граждан. Среди них следует выделить ряд федеральных законов Российской Федерации: «О связи» (№ 126-ФЗ от 7 июля 2003 года), «Об информации, информационных технологиях и о защите информации» (№ 149-ФЗ от 27 июля 2006 года); «О защите детей от информации, причиняющей вред их здоровью и развитию» (№ 436-ФЗ от 29.12.2010); «О внесении изменений в федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации» (№ 139-ФЗ от 28 июля 2012 года). Однако, к сожалению, этого недостаточно для полноценной защиты населения от разнообразных форм киберпреступности в Интернет-пространстве.

Таким образом, опираясь на опыт зарубежных стран, предлагаем ряд практических рекомендаций по защите от кибersталкинга: незамедлительное выдвижение кибersталкеру требования о прекращении кибератак; сохранение всех электронных сообщений, видеоматериалов, содержащих угрозы и их резервных копий; обращение к Интернет-провайдеру с просьбой прекратить поступающие киберугрозы; обращение в полицию; ведение детального учета контактов с Интернет-провайдером и сотрудниками правоохранительных органов [11].

Для повышения уровня личной безопасности необходимо соблюдать ряд основных правил в сети Интернет: использовать надежные пароли; не применять одни и те же учетные данные или пароли повторно; не отправлять важную информацию через социальные сети; использовать настройки конфиденциальности на сайтах социальных сетей только для друзей и знакомых; следить за изменениями в уровнях

политики конфиденциальности, периодически просматривая настройки конфиденциальности и безопасности; по возможности ограничить свои личные публикации в Интернет-ресурсах; вдумчиво писать комментарии, избегая негативных высказываний.

Библиографические ссылки

1. Барышева К.А. Преследование как новый вид уголовно-наказуемого деяния // Пробелы в российском законодательстве. 2016. № 8. С. 178-183.
2. В Норвегии законодательно запретили сталкинг [Электронный ресурс] : [сайт]. – URL: https://scandinews.fi/society/2021-v-norvegii-zakonodatelno-zapretili-stalking (дата обращения: 12.03.2020).
3. Ривман Д. В.Криминальная виктимология. – СПб.: Питер, 2002. – 304 с.
4. Франк Л.В. Виктимология и виктимность. Об одном новом направлении в теории и практике борьбы с преступностью: Учебное пособие / Франк Л.В.; Отв. ред.: Муллаев М.М. – Душанбе, 1972. – 113 с.
5. Anderson, M., & Jiang, J. Teens, social media, and technology, Washington, DC: Pew Research Center. 2018. Электронный ресурс] : [сайт]. – URL: https://www.pewinternet.org/wpcontent/uploads/sites/9/2018/05/PI_2018.05.31_TeensTech_FINAL.pdf (дата обращения: 13.03.2020).
6. Breiding M.J., Smith S.G., Basile K.C., Walters M.L., Chen J., Merrick M.T. Prevalence and characteristics of sexual violence, stalking, and intimate partner violence victimization--national intimate partner and sexual violence survey, United States, 2011 [Электронный ресурс] // Morbidity and mortality weekly report. Surveillance summaries Surveill Summ. 2014. № 63(8). Pp.1-18. URL: https://www.cdc.gov/mmwr/preview/mmwrhtml/ss6308a1.htm (дата обращения: 12.03.2020).
7. Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws [Электронный ресурс] : [сайт]. – URL: https://scholarship.law.missouri.edu/cgi/viewcontent.cgi?referer=https (дата обращения:.
8. Cyberstalking: The Law Dictionary for Everyone [Электронный ресурс] : [сайт]. – URL: https://legaldictionary.net/cyberstalking/ (дата обращения: 14.03.2020).
9. Kowalski R.M., Limber S.P., & Agatston P.W. Cyberbullying: Bullying in the digital age (2nd ed.) // Psychological Bulletin. 2014. Vol.140. № 4. Pp. 1073-1137.
10. McFarlane L., Bocij P. An Exploration of Predatory Behaviour in Cyberspace: Toward a Typology of Cyberstalkers [Электронный ресурс] : [сайт]. – URL: https://firstmonday.org/ojs/index.php/fm/article/view/1076/996 (дата обращения: 15.03.2020).
11. Trolling, Doxing & Cyberstalking: Cybercrime & The Law. Cybercrime is one of the greatest threats facing US with implications for national security. [Электронный ресурс] : [сайт]. – URL: https://securityaffairs.co/wordpress/56841/laws-and-regulations/trolling-doxing-cyberstalking-cybercrime-law.html (дата обращения: 15.03.2020).