V

УДК 343.988 Виктимология 2021, Т. 8, № 2. С. 143–148

К вопросу о виктимизации жертв киберпреступлений

Хоменко А. Н.
Сибирский институт бизнеса и информационных технологий
г. Омск, Российская Федерация
E-mail: an.homenko65@mail.ru.

Аннотация. Актуальность рассматриваемой в статье проблемы состоит в том, что многие аспекты жизнедеятельности человека в современном обществе осуществляются в цифровом формате. При этом преступность, как атрибут социума, показывает эффективность своих криминальных деяний, используя тот же инструмент IT-технологий. Статистические данные и ведомственные показатели преступности правоохранительных органов за последние три года показывают, что наибольшую угрозу и вред от киберпреступлений общественным отношениям, обеспечивающим охрану прав и свобод личности, собственности граждан, представляют кибермошенничество и кибербуллинг.

В представленном вашему вниманию исследовании, автор, попытался определить виктимологические детерминанты, которые способствуют виктимизации жертв данных посягательств. Указать на особенности причин их виктимного поведения непосредственно связанных с личностью потерпевшего, мотивацией его поведения и конкретной жизненной ситуацией (пандемией). В завершении работы сделан акцент на основные меры, способствующие девиктимизации жертв деяний, совершенных с помощью средств информационно-телекоммуникационных технологий.

Ключевые слова: виктимизация, киберпреступление, сеть «Интернет», жертва, мошенничество, пандемия.

Для цитирования: Хоменко, А. Н. К вопросу о виктимизации жертв киберпреступлений / А. Н. Хоменко // Виктимология. — 2021. — Т. 8, № 2. — С. 143–148.

On the Victimization of Cybercrime Victims

A. N. Khomenko
Siberian Institute of Business and Information Technologies
Omsk, Russian Federation
E-mail: an.homenko65@mail.ru.

Abstract. The relevance of the problem considered in the article is that many aspects of human life in modern society are carried out in a digital format. At the same time, crime, as an attribute of society, shows the effectiveness of its criminal acts, using the same tool of IT-technology. Statistical data and departmental indices of law-enforcement agencies over the last three years demonstrate that cybercrime and cyberbullying pose the greatest threat and harm to social relations, which ensures protection of rights and freedoms of individuals and citizens' property. In the study presented to your attention, the author tried to identify the victimological determinants that contribute to victimization of victims of these attacks. Point out the peculiarities of the causes of their victimization behavior directly related to the personality of the victim, the motivation of his/her behavior and the specific life situation (pandemic).

At the end of the paper, the emphasis is placed on the main measures that contribute to the de-victimization of victims of acts committed by means of information and telecommunication technologies.

Keywords: victimization, cybercrime, Internet, victim, fraud, pandemic.
For citation: Khomenko, A. N. On the Victimization of Cybercrime Victims. *Viktimologiya* [Victimology], 2021, vol. 8, no. 2, pp. 143-148. (In Russ.)

Введение

В настоящее время человечество переживает быстрый перевод различных сфер жизнедеятельности в сеть «Интернет», включая оборот безналичных денежных средств, а также неконтролируемые государством финансовые взаиморасчеты в виртуальной (цифровой) валюте — блокчейн-технологии, типа биткойна и т. п. «Информационное общество характеризуется активным внедрением информационных технологий в различные сферы деятельности и быта человека и образованием информационного пространства, называемого киберпространством» [1, с. 78]. По данным Росстата, цифровизация услуг в стране приобретает лавинообразный характер революции: в 2010 году 48 % россиян пользовались интернет-услугами, в 2018 — 59 %, в 2020 году — 72 % (в городах-миллионниках — 95 %)[1].

Описание исследования

Как известно, преступность всегда идет в ногу со временем, следовательно, вместе с позитивным цифровым развитием общественных отношений фиксируется ее существенный рост с использованием современных IT-технологий в криминальных целях. «Преступность необратимо уходит и действует через киберпространство. При этом не обязательно, чтобы само преступление совершалось в виртуале. С появлением «интернета всего» киберпространство все чаще используется для совершения традиционных преступлений при помощи нетрадиционных орудий и методов» [7, с. 104]. Таким образом, в данном исследовании представляется возможным определить понятие «киберпреступление», как посягательство на охраняемое уголовным законом общественное отношение, совершенное посредством информационно-телекоммуникационных технологий либо в киберпространстве.

Указанную тенденцию подтверждают данные состояния преступности в Российской Федерации. Так, в 2019 год было зарегистрировано 294,4 тысячи преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Удельный вес преступлений с использованием IT-технологий увеличился с 8,8 % в 2018 г. до 14,5 % в 2019 г. При этом почти половина всех зафиксированных киберпреступлений (48,5 %) относилось к категориям тяжких и особо тяжких, что на 149 процентов больше, чем в 2018 году[2].

За 2020 год было зарегистрировано уже 510,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или на 73,4 % больше, чем за аналогичный период 2019 года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 14,5 % до 25,0 %. Больше половины таких преступлений (52,4 %) относится к категориям тяжких и особо тяжких: 267,6 тыс. (+87,5 %); больше половины (58,8 %) совершается с использованием сети «Интернет»: 300,3 тыс. (+91,3 %), почти половина (42,9 %) — средств мобильной связи: 218,7 тыс. (+88,3 %). Четыре таких преступления (80,4 %) из пяти совершаются путем кражи или мошенничества: 410,5 тыс. (+74,3 %), почти каждое одиннадцатое (9,2 %) — с целью незаконного производства, сбыта или пересылки наркотических средств: 47,1 тыс. (+90,7 %)[3].

[1] Как остановить унижения и издевательства в Сети // Российская газета : [сайт]. — URL: https://rg.ru/2021/02/03/kak-ostanovit-unizheniia-i-izdevatelstva-v-seti.html (дата обращения: 07.02.2021).

[2] Резко выросло число преступлений, совершаемых с помощью IT-технологий // Российская газета : [сайт]. — URL: https://rg.ru/2020/01/28/rezko-vyroslo-chislo-prestuplenij-sovershaemyh-s-pomoshchiu-it-tehnologij.html (дата обращения: 07.02.2021).

[3] Состояние преступности в Российской Федерации за янв.-дек. 2020 г. Москва, ГИАЦ МВД России. С. 4.

Вместе с тем данную динамику преступности обострило и введение в России с марта 2020 г. особых карантинных условий, вызванных пандемией COVID-19. Введенный режим ограничивает права граждан, прежде всего, на свободу передвижения. Поэтому многие из них были вынуждены оставаться в местах проживания (пребывания) и выполнять требования строгой самоизоляции. В такой обстановке «…формы социально-психологического состояния людей во многих случаях обладают, как об этом свидетельствуют результаты криминологических исследований, значительным криминогенным потенциалом и в отсутствии должного контроля нередко разрешаются противоправным способом, в том числе путем совершения преступлений» [4, с. 44].

В докладе, представленном в октябре 2020 года на международном форуме Академии Управления МВД РФ «Стратегическое развитие системы МВД России: состояние, тенденции, перспективы», главным выводом исследования назван стремительный рост компьютерной преступности, в первую очередь, финансовых мошенничеств с использованием социальной инженерии — вишинга, фишинга — жертвами которых становились, в основном, клиенты банков. Активно использовалась эксплуатация темы COVID-19 во вредоносных рассылках, переключение операторов вирусов-шифровальщиков на крупные цели, а также усилился рекрутинг в преступные сообщества новых участников. Было отмечено, что суммарно за 9 месяцев 2020 года CERT-GIB заблокировал 14 802 фишинговых ресурса, нацеленных на хищение денег и персональной информации посетителей сайтов (логины, пароли от аккаунтов и интернет-банков, данные банковских карт). Это больше, чем за весь 2019 год, когда были заблокированы 14 093 таких веб-ресурсов[1].

Кроме того, данная пандемия связана с распространением инфекции в мировом масштабе. В частности, учитывая рекордное число потенциальных жертв, которые остаются дома и пользуются онлайн-услугами в Европейском союзе, способы использования киберпреступниками появляющихся при этом возможностей и уязвимостей возросли. Оценка зарегистрированных преступлений Европолом[2] позволила сделать вывод, что режим карантина особенно отразился на росте киберпреступности, торговли контрафактными и некачественными товарами, а также различных видов мошенничества и схем, связанных с организованной преступностью [3, с. 39].

Вышеизложенное состояние преступности указывает, что наиболее распространенным деянием в сети «Интернет» является кибермошенничество. Большой интерес к промыслу обмана в сети «Интернет» связан с возможностью киберпреступников анонимно из любой точки мира совершать деяния против собственности граждан любой страны. При этом жертвы компьютерного мошенничества в большинстве случаев (70,3 %) не знакомы с жертвой.

В рамках заявленной темы, прежде чем понять особенности виктимизации жертвы данного преступления, необходимо определить виктимилогические детерминанты кибермошенничества, которые непосредственно связаны с личностью потерпевшего, мотивацией его поведения и конкретной жизненной ситуацией. В ходе психологического исследования были выделены два основных типа виктимного поведения, присущего жертвам Интернет-мошенничества. Первым типом является активное поведение, провоцирующее преступление своими действиями — просьбой или обращением. Вторым — агрессивное поведение, провоцирующее преступное действие оскорблениями, клеветой, издевательством и т. п. [6, с. 82]

Поведение жертвы в механизме совершения мошенничества было реализацией виктимогенной деформации личности, выраженной в неправомерных действиях

[1] Эксперты назвали тенденции киберпреступлений в период пандемии // Российская газета : [сайт]. — URL: https://rg.ru/2020/10/23/eksperty-nazvali-tendencii-kiberprestuplenij-v-period-pandemii.html (дата обращения: 07.02.2021).

[2] Европол — полицейская служба Европейского союза. Основными задачами службы являются координация работы национальных служб в борьбе с международной организованной преступностью и улучшение информационного обмена между национальными полицейскими службами.

в 12,6 % случаев. Треть потерпевших (33,3 %) вели себя неосмотрительно вследствие излишней доверчивости, некритичности, суеверия [5]. Так, обоснованный вывод, сделанный А. В. Майоровым и Н. Е. Яременко, указывает на то, что мошенники, выбирая потенциальную жертву, изучают ее объективные (внешние) признаки — пол, возраст и образование, а также субъективные — психическая устойчивость, доверчивость, мнительность, способность прийти на помощь, алчность и т. п. Например, милосердные люди, сострадающие больным детям, животным и иным нуждающимся становятся легкой «мишенью» различного рода размещений, «благотворительных акций» в интернете [2, с. 38]. Доминантой причин виктимизации, рассматриваемой жертвы, является невежество в использовании средств информационно-телекоммуникационных технологий и нерациональная доверительность, основанная на их самоуверенности и самонадеянности.

Процесс виктимизации жертв кибермошенничества был проанализирован центром исследования «Internet Fraud Complaint Center». В результате выяснилось, что почти 43 % всех случаев мошенничества, зафиксированных в последние годы, произошло именно с участниками аукционов. Каждый пятый потерпевший (18–22 %) был обманут нечестными продавцами товаров и услуг, а около 15 % инцидентов было связано с так называемыми «нигерийскими письмами» (предложениями о помощи в вывозе за пределы страны крупных денежных сумм). И только в 1,4 % криминальных ситуаций виновными оказывались предприятия электронной торговли. Мужчины становятся жертвами подобных преступлений чаще, чем женщины, а пожилые люди чаще, чем молодые по причине, прежде всего, непринятия мер по защите своих персональных систем. Так, 73,8 % жертв не использовали технические средства по защите информации и для мониторинга незаконного проникновения[1].

Еще одним немаловажным триггером виктимизации несовершеннолетних в сети «Интернет» является кибербуллинг (кибермоббинг), учитывая то, что коммуникация между ними все больше происходит, к сожалению, только в виртуальном пространстве. В тоже время следует отметить, что по статистике Роскомнадзора, в год выявляется более 100 тыс. случаев распространения противоправной информации в социальных сетях, и этот показатель растет. В этом ведомстве привели в пример треш-стриминги, когда в прямом эфире блогеры принимают запрещенные вещества, избивают друг друга и т. п.[2]

При совершении кибербуллинга речь идет о ситуациях, когда подростки используют современные технологии для того, чтобы пугать, притеснять, унижать или иным способами вызывать беспокойство у сверстников, рассылая обидные письма, распространяя сплетни, создавая веб-страницы, видео и профили в социальных сетях, чтобы над кем-то посмеяться, делая фотоснимки там, где люди рассчитывают на уединение, и распространяя их онлайн, без разрешения снимая и загружая в сеть видеоматериалы, используя анонимные приложения для унижения и разрушения достижений игроков в игровых сетях и пр. [8, с. 278] Так, в отчете российского Фонда развития Интернета указано, что практически каждый третий подросток за год использования интернета сталкивался с коммуникационными рисками, среди которых лидировал кибербуллинг, а каждый четвертый — сталкивался с оскорблениями, унижениями или преследованием в сети[3]. Результатом такого психологического давления, связанного с негативными переживаниями (злость, фрустрация, депрессия, страх) не редко возникают последствия в виде самоповреждения, суицида жертвы

[1] Федоренко В. Виктимологический аспект преступлений в сети Интернет // Портал «zakon.ru». — URL: https://zakon.ru/blog/2012/01/19/viktimologicheskij_aspekt_prestuplenij_v_seti_internet (дата обращения: 07.02.2021).

[2] Соцсетям с 1 февраля придется блокировать запрещенный контент // Российская газета : [интернет-портал]. — URL: https://rg.ru/2020/12/23/socseti-s-1-fevralia-obiazali-blokirovat-zapreshchennyj-kontent.html (дата обращения: 07.02.2021).

[3] Солдатова Г. У., Нестик Т. А., Рассказова Е. И., Зотова Е. Ю. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования. Москва : Фонд Развития Интернет, 2013. — URL: http://detionline.com/assets/files/research/DigitalLiteracy.pdf (дата обращения: 07.02.2021).

или ответной агрессивной реакции со стороны родителей несовершеннолетних (виновного лица и жертвы) с нанесением телесных повреждений (причинением смерти).

Итак, причины и процесс виктимизации вышеуказанных отдельных видов киберпреступлений, позволяют определить некоторые меры их девиктимизации, влияющие на ограничение киберугроз для российского общества. К таким мерам в настоящее время следует отнести создание специальных структур МВД России для борьбы с киберпреступлениями. При этом запланировано существенно увеличить штат Бюро специальных технических мероприятий, отвечающих за использование полицейскими различных технических устройств и гаджетов ведомства на региональном уровне[1].

Также с 1 февраля 2021 года интернет-ресурсы, согласно внесенным изменениям в Федеральный закон «Об информации, информационных технологиях и о защите информации» (в части установления особенностей распространения информации в социальной сети)[2], должны самостоятельно выявлять и блокировать незаконный общественно-опасный контент: материалы с порнографическими изображениями несовершеннолетних; информацию, склоняющую детей к совершению опасных незаконных действий; о способах совершения самоубийства и призывах к нему; об изготовлении и использовании наркотиков; информацию, которая в неприличной форме оскорбляет человеческое достоинство и общественную нравственность; с призывами к массовым беспорядкам, экстремизму, терроризму и участию в несогласованных публичных мероприятиях.

Заключение

В завершении следует подчеркнуть, что масштабирование активного виктимного поведения пользователей средствами информационно-телекоммуникационных технологий, требует от субъектов государственной (муниципальной) власти и общественных организаций, оперативных мер виктимологической профилактики киберпреступлений, направленных, прежде всего, на индивидуальное воспитание несовершеннолетних, повышение уровня правосознания и технического образования в сфере кибербезопасности россиян.

[1] Резко выросло число преступлений, совершаемых с помощью IT-технологий // Российская газета : [сайт]. — URL: https://rg.ru/2020/01/28/rezko-vyroslo-chislo-prestuplenij-soversh aemyh-s-pomoshchiu-it-tehnologij.html (дата обращения: 07.02.2021).

[2] О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» : законопроект № 223849-7 // СОЗД ГАС «Законотворчество». — URL: https://sozd.duma.gov.ru/bill/223849-7 (дата обращения: 07.02.2021).

СПИСОК ЛИТЕРАТУРЫ

1. Буз, С. И. Киберпреступления: понятие, сущность и общая характеристика / С. И. Буз // ЮристЪ-Правоведъ. — 2019. — № 4 (91). — С. 78–82.

2. Майоров, А. В. Виктимологический аспект мошенничества / А. В. Майоров, Н. Е. Яременко // Виктимология. — 2019. — № 3 (21). — С. 36–41.

3. Мартыненко, Н. Э. Влияние COVID-19 на изменение уголовного закона и состояние преступности / Н. Э. Мартыненко // Российский следователь. — 2020. — № 9. — С. 37–40.

4. Мусеибов, А. Г. Влияние образа жизни населения в период пандемии коронавирусной инфекции на состояние и динамику преступности / А. Г. Мусеибов, А. В. Борбат // Российский следователь. — 2020. — № 9. — С. 41–45.

5. Рогова, Е. В. Роль виктимного поведения потерпевших в механизме совершения преступлений / Е. В. Рогова // Известия иркутской государственной экономической академии (Байкальский государственный университет экономики и права). — 2011. — № 2. — URL: https://cyberleninka.ru/article/n/rol-viktimnogo-povedeniya-poterpevshih-v-mehanizme-sovershe niya-prestupleniy (дата обращения: 02.02.2021).

6. Сафуанов, Ф. С. Особенности личности жертв противоправных посягательств в Интернете / Ф. С. Сафуанов, Н. В. Докучаева // Психология и право. — 2015. — Т. 5, № 4. — С. 80–93.

7. Сборник избранных лекций по криминологии : учебное пособие / под. ред. д-ра юрид. наук проф. Т. В. Пинкевич. — Москва : Юрлитинформ, 2020. — 392 с.

8. Хломов, К. Д. Кибербуллинг в опыте российских подростков / К. Д. Хломов, Д. Г. Давыдов, А. А. Бочавер // Психология и право. — 2019. — № 2 (9). — С. 276–295.

REFERENCES

1. Buz S. I. *Kiberprestupleniya: ponyatie, sushchnost' i obshchaya harakteristika* [Cybercrime: Concept, Essence and General Characteristics], *Yurist-Pravoved,* 2019, no. 4 (91), pp. 78–82. (In Russ.).

2. Majorov A. V., Yaremenko N. E. *Viktimologicheskij aspekt moshennichestva* [The Victimological Aspect of Fraud], *Viktimologiya*, 2019, no. 3 (21), pp. 36–41. (In Russ).

3. Martynenko N. E. *Vliyanie COVID-19 na izmenenie ugolovnogo zakona i sostoyanie prestupnosti* [The Impact of COVID-19 on Changing Criminal Law and Crime], *Rossijskij sledovatel'*, 2020, no. 9, pp. 37–40. (In Russ.).

4. Museibov A. G. *Vliyanie obraza zhizni naseleniya v period pandemii koronavirusnoj infekcii na sostoyanie i dinamiku prestupnosti* [The Impact of Lifestyles during the Coronavirus Pandemic on the Status and Dynamics of Crime], *Rossijskij sledovatel'*, 2020, no. 9. pp. 41–45. (In Russ.).

5. Rogova E. V. *Rol' viktimnogo povedeniya poterpevshih v mekhanizme sovershenija prestuplenij* [The Role of Victim Behavior in the Mechanism of Crime]. *Baikal Research Journal*, 2011, no. 2. Available at: https://cyberleninka.ru/article/n/rol-viktimnogo-povedeniya-poterpevshih-v-mehanizme-sovershenija-prestupleniy (accessed 2 Feb 2021). (In Russ.).

6. Safuanov F. S. *Osobennosti lichnosti zhertv protivopravnyh posyagatel'stv v Internete* [Characteristics of the personality of victims of unlawful encroachments on the Internet], *Psihologiya i pravo*, 2015, vol. 5, no. 4, pp. 80–93. (In Russ.).

7. *Sbornik izbrannyh lekcij po kriminologii* [A Collection of Selected Lectures on Criminology], Moscow, YUrlitinform Publ., 2020, 392 p. (In Russ).

8. Hlomov K. D., Davydov D. G., Bochaver A. A. *Kiberbulling v opyte rossijskih podrostkov* [Cyberbullying in the Experience of Russian Teenagers], *Psihologiya i pravo*, 2019, no. 2 (9), pp. 276–295. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Хоменко Анатолий Николаевич, кандидат юридических наук, доцент, Сибирский институт бизнеса и информационных технологий, ул. 24-я Северная, д. 196/1, г. Омск, 644116, Российская Федерация; e-mail: an.homenko65@mail.ru, SPIN-код: 3269-9778, Author ID: 688662.

INFORMATION ABOUT THE AUTHOR

Anatoly N. Khomenko, Candidate of Law Sciences, Associate Professor, Siberian Institute of Business and Information Technology, 196/1 24 Severnaya St., Omsk 644116, Russian Federation; e-mail: an.homenko65@mail.ru, SPIN code: 3269-9778, Author ID: 688662.

Дата поступления в редакцию / Received: 08.02.2021.