КИБЕРПРЕСТУПНОСТЬ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НЕСОВЕРШЕННОЛЕТНИХ

Симонова С.С.
Волгоградский институт управления – филиал РАНХиГС, г. Волгоград
email: simonova.ss@mail.ru

Аннотация. Обеспечение информационной безопасности детей и подростков является актуальной задачей и важным направлением информационной политики России и мира. Рост киберпреступлений неминуемо порождает новые угрозы информационной безопасности несовершеннолетних. Автор приходит к выводу, что всестороннее изучение и анализ факторов, способствующих виктимизации подростков, позволяет минимизировать кибер-угрозы в отношении несовершеннолетних и проводить эффективную профилактику киберпреступлений, совершаемых в отношении несовершеннолетних.

Ключевые слова: кибербезопасность, информационная безопасность, кибер-угрозы, киберпреступность, информационная безопасность несовершеннолетних, кибербуллинг, информационная политика, несовершеннолетние.

Современную жизнь уже невозможно представить без информационно-телекоммуникационных систем. Растущее разнообразие технических устройств, которые позволяют получить доступ к сети Интернет, способствовало общему росту пользователей Интернета в самых разных местах и обстоятельствах. Эти устройства стали частью нашей жизни, и мы используем их для достижения различных целей [1, с. 1849]. Наибольшей популярностью пользуется Интернет у подростков, которые активно общаются в популярных мессенджерах, просматривают видеоролики и ищут информацию для учебы в Сети Интернет. К примеру, в Великобритании 83% подростков в возрасте от 12 до 15 лет владеют смартфонами, и 99% несовершеннолетних проводят в среднем 20,5 часов в неделю в Интернете [2].

Детская аудитория российского Интернета насчитывает 8–10 млн. пользователей до 14 лет – это около половины всех детей, проживающих в России. При этом около 40% детей, регулярно посещающих сеть, просматривают Интернет-сайты с агрессивным и нелегальным контентом, подвергаются кибер-преследованиям и виртуальным домогательствам. [3, с. 87]

Использование Интернета как части нашей повседневной жизни принесло много преимуществ, а также облегчило наш образ жизни. Действия, которые раньше требовали часов или дней для решения, например, отправка корреспонденции, были сокращены до минимального времени [4, с. 1061].

При всех достоинствах использования Интернета (быстрота и легкость поиска информации, мгновенная ее передача в любую точку мира, возможность хранения и передачи огромного объема информации и т.д.), с каждым годом мы наблюдаем всё возрастающее разнообразие киберугроз.

Обращаясь к статистическим данным, следует отметить, что в 2020 число киберпреступлений значительно возросло. Так, на официальном сайте Министерства внутренних дел Российской Федерации опубликована Краткая характеристика состояния преступности в Российской Федерации за январь - сентябрь 2020 года. Согласно данным статистики, «общее число зарегистрированных в стране преступлений увеличилось на 1,2%. Это обусловлено, главным образом, ростом количества криминальных деяний с применением IT-технологий. В отчетном

периоде их совершено на 77% больше, чем год назад, в том числе с использованием сети «Интернет» – на 93,2%, при помощи средств мобильной связи – на 97,7%»[1].

Следует обратить внимание на такую закономерность: по мере увеличения числа пользователей, ставших жертвами кибератак, возрастает и общая обеспокоенность по поводу киберпреступности. Традиционно киберпреступность понимается как совокупность действий, при которых для совершения преступления используются компьютерные технологии [5].

Растущий список киберпреступлений включает как преступления, которые стали возможными только благодаря компьютерам и всемирной Сети (это такие преступные деяния, как сетевые вторжения и распространение компьютерных вирусов), а также компьютерные кибер-вариации преступлений, давно существующих не в виртуальном, а в реальном мире (например, таких как клевета, кража личных данных, вымогательство, мошенничество, террористические атаки).

Преступники во всемирной паутине используют личную информацию пользователей Интернета в своих интересах [6, с. 730].

В последнее время по мере развития искусственного интеллекта мир сталкивается с новой проблемой - киберпреступностью на основе искусственного интеллекта, которая становится продуктом технологического развития, создавая угрозу национальной и общественной безопасности, защите прав граждан на собственность и неприкосновенность частной жизни [7].

Совершение указанных преступлений посредством Сети Интернет в последнее время получает всё большее распространение и становится серьезной проблемой не только для пользователей конкретной страны, но и для всего мирового сообщества. В связи с этим Европейский Союз призывает прикладывать все усилия по обеспечению защиты от киберугроз как на нормативном-правовом, так и на стратегическом уровнях.

Как известно, несовершеннолетние являются наиболее уязвимой категорий пользователей сети Интернет. Это обусловливается еще не созревшей психикой подростков, их склонностью к доверию. Как следствие, несовершеннолетние часто становятся жертвами киберпреступлений, а также разнообразных киберугроз, таких как фишинг, кибербуллинг, склонение к насилию, употреблению наркотиков и суициду. В связи с этим обеспечение информационной безопасности несовершеннолетних (под которой, согласно ст. 2 Федерального закона "О защите детей от информации, причиняющей вред их здоровью и развитию", понимается состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию[2]), является актуальной задачей, для достижения которой важно учитывать ряд факторов.

Среди указанных факторов, по нашему мнению, важную роль играет изучение виктимности подростков, то есть подверженности подростков стать жертвой киберпреступлений. Рассмотрим факторы виктимности для несовершеннолетних.

Существуют исследования, согласно которым частое использование в повседневной жизни Сети Интернет связано с большей вероятностью виктимизации потенциальных жертв киберпреступлений [8]. При этом существует прямая зависимость: чем большую онлайн-активность проявляют несовершеннолетние интернет-пользователи, тем больше они способствуют своей виктимизации

[1] Краткая характеристика состояния преступности в Российской Федерации за январь - сентябрь 2020 года / Официальный сайт МВД России [Электронный ресурс]: Режим доступа: https://xn--b1aew.xn--p1ai/reports/item/21551069/ (дата обращения: 27.11.2020).

[2] Федеральный закон от 29.12.2010 N 436-ФЗ (ред. от 31.07.2020) "О защите детей от информации, причиняющей вред их здоровью и развитию"/ СПС Консультант плюс: http://www.consultant.ru/document/cons_doc_LAW_108808/ (дата обращения: 25.11.2020).

посредством онлайн-деятельности. Кроме того, киберугрозу зачастую может создавать использование небезопасных подключений к Интернету.

Как добровольное, так и принудительное раскрытие личной информации через сайты социальных сетей и веб-сайты с онлайн-рекламой повышает вероятность того, что указанные данные станут целью фишинга [9, с. 1668]. Сообщение подростками персональных данных, причем как своих, так и членов их семьи, предполагает участие в онлайн-форумах и онлайн-играх, обмен личной информацией в социальных сетях и мессенджерах, доступ к контенту для взрослых.

Еще одним фактором виктимизации несовершеннолетних является такая черта, проявляемая в общении со сверстниками, неправильное истолкование подшучивания онлайн, невозможность отличить юмор от кибербуллинга (киберзапугивания). Под кибербуллингом принято понимать психологическое насилие среди школьников, осуществляемое посредством сети Интернет.

В отличие от традиционного буллинга (травли, запугивания), все действия, унижающие подростков, происходят в виртуальном пространстве, с помощью информационных и коммуникационных технологий.

Представляет интерес исследование, направленное на изучение взглядов и представлений подростков о роли юмора и подшучивания в киберзапугивании [2]. Согласно проведенному среди семи фокус-групп с участием 28 учащихся средних школ (20 девушек, 8 молодых людей) в возрасте от 11 до 15 лет, подростки разделяют понимание агрессивного поведения в Интернете, например, шуток в Интернете, которые описывают их как неоднозначные и трудно поддающиеся интерпретации. Участники продемонстрировали понимание того, как неоднозначность, вызванную онлайн-средой в сочетании с подшучиванием, можно интерпретировать как предполагаемое или полностью признанное киберзапугивание.

В этом контексте подростки могут стать как жертвой описываемой киберугрозы, так и её источником, иначе говоря, субъектом кибербуллинга. Согласно опросам жертв кибербуллинга, они испытывают негативные эмоциональные последствия, такие как гнев, разочарование, грусть, чувство крайнего расстройства, испуга и смущения. У несовершеннолетних жертв кибербуллинга чаще всего встречаются такие симптомы как тревога, стресс, занижение самооценки и даже мысли о суициде.

Следовательно, есть веские основания предполагать, что быть объектом кибербуллинга разрушительно и психологически вредно для несовершеннолетних. В этом контексте особую значимость приобретает профилактика кибербуллинка, включающая в себя получение подробных сведений о поведении подростков в Интернете в отношении ровесников. Это позволит специалистам-практикам снижать уровень виктимности в отношении киберзапугивания.

Следующим фактором виктимности подростков в сети Интернет является их нежелание сообщать кому бы то ни было о киберпреступлении, совершенном в отношении несовершеннолетнего. Это обстоятельство, во-первых, не позволяет оказывать подросткам социальную и правовую поддержку, и во-вторых, способствует повышению уровня латентности киберпреступлений. Следует особо отметить, что и расследование киберпреступлений представляет особую сложность из-за анонимности как свойства Интернет-пространства, которым пользуются киберпреступники. В связи с этим представляется необходимым совершенствования информационной политики в русле повышения информационной грамотности подростков. Речь идет, в том числе, об информировании несовершеннолетних о ресурсах, позволяющих сообщить о киберпреступлении анонимно (горячая линия, анонимный звонок, форум для жертв киберугроз и т.п.). Определенные шаги в этом направлении уже сделаны. Так, В 2008 году был создан Национальный Узел

Интернет-безопасности в России (в настоящее время является Интернет-СМИ «Центр безопасного Интернета в России»). На данном сайте для подростков есть Горячая линия и Линия помощи жертвам кибер-угроз. Также в рамках проекта «Дети онлайн» разработаны материалы, посвященные безопасному поведению в Интернете.

С 2012 года Координационным центром национальных доменов .RU и .РФ при поддержке ПАО «Ростелеком» реализуется социально-образовательный проект для школьников «Изучи Интернет – управляй им». Целью этого проекта является повышение уровня цифровой грамотности несовершеннолетних пользователей Интернет в современной интерактивной форме. Центр бесплатной правовой помощи (юридическая клиника) Волгоградского института управления – филиала РАНХиГС проводит на регулярной основе занятия по правовому просвещению на базе школ для учеников разных классов, а также на базе Волгоградской областной библиотеки для молодежи.

Таким образом, компьютерная сеть расширяется день ото дня, и количество пользователей в сети, особенно подростков увеличивается [10, с. 149]. В сети существует множество атак, которые ставят информационную безопасность несовершеннолетних пользователей под угрозу. Особого внимания заслуживает такая проблема, как обеспечение информационной безопасности детей и подростков.

Именно несовершеннолетние чаще подвергаются негативному воздействию в сети Интернет, они рискуют стать жертвами кибербуллинга, мошенничества и неправомерного доступа к личной информации. Среди распространенных угроз информационной безопасности несовершеннолетних также можно выделить постоянное увеличение количества интернет-сайтов с агрессивным или нелегальным контентом, в том числе призывающих к суициду и склоняющих к употреблению наркотических средств и психотропных веществ, а также осуществление посредством сети Интернет киберпреследований и виртуальных домогательств [11, с. 234].

К важнейшим социальным мерам обеспечения информационной безопасности несовершеннолетних относятся, в первую очередь, создание и внедрение программ обучения детей и подростков правилам безопасного поведения в Интернет-пространстве, профилактика интернет-зависимости, предупреждение рисков вовлечения в противоправную деятельность.

Следовательно, для обеспечения информационной безопасности детей и подростов необходимо комплексное применение правовых, технических и социальных мер профилактики киберпреступлений.

Библиографический список

1. Carvalho, J.V., Carvalho, S., Rocha, Á. European strategy and legislation for cybersecurity: implications for Portugal // Cluster Computing. – 2020. - 23(3). - pp. 1845-1854.

2. Oonagh L.Steer, Lucy R.Betts, Thomas Baguley, Jens F.Binder. «“I feel like everyone does it”- adolescents' perceptions and awareness of the association between humour, banter, and cyberbullying» // Computers in Human Behavior. - 2020. – Vol. 108. – Art. 106297

3. Хохлова Н.И, Обеспечение детской безопасности в Интернете: российский опыт и зарубежные инициативы // Пространство и Время. - 2012. - №1. – С. 87-91.

4. Boussi, G.O., Gupta, H. A Proposed Framework for Controlling Cyber-Crime // 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions).- 2020. – Vol. 9197975.- p. 1060-1063.

5. Chandra, A., Snowe, M.J. A taxonomy of cybercrime: Theory and design // International Journal of Accounting Information Systems. – 2020. - № 38. – Art. 100467.
6. Zeid, R.B., Moubarak, J., Bassil, C. Investigating the Darknet // International Wireless Communications and Mobile Computing, IWCMC. – 2020. - Volume 9148422. - pp. 727-732.
7. Wang, X. Criminal Law Protection of Cybersecurity Considering AI-based Cybercrime // Journal of Physics: Conference Series. – 2020. - № 1533(3). – Art. 032014.
8. Cheng, C., Chan, L., Chau, C.-L. Individual differences in susceptibility to cybercrime victimization and its psychological aftermath // Computers in Human Behavior. - 2020 . – Volume 108. – Art. 106311.
9. Akdemir, N., Lawless, C.J. Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: a lifestyle routine activities approach // Internet Research. – 2020. - 30(6). - pp. 1665-1687.
10. Srivastava U., Sharma N. Artificial Neural Network-Based Bilevel Prediction Model for Rare Attack Detection // International Conference on Computational Performance Evaluation. – 2020. – pp. 146-152.
11. Миронова С.М.. Симонова С.С. Защита прав и свобод несовершеннолетних в цифровом пространстве // Всероссийский криминологический журнал. – 2020. – Том 14. – №2. – С. 234-241.

CYBER CRIME AND INFORMATION SECURITY FOR MINORS

Simonova S.S.
Volgograd Institute of Management - branch of RANEPA, Volgograd
email: simonova.ss@mail.ru

Abstract. Ensuring information security for children and adolescents is an urgent task and an important area of information policy in Russia and the world. The growth of cybercrimes inevitably generates new threats to the information security of minors. The author comes to the conclusion that a comprehensive study and analysis of the factors contributing to the victimization of adolescents makes it possible to minimize cyber threats against minors and to carry out effective prevention of cybercrimes committed against minors.

Keywords: cybersecurity, information security, cyber threats, cybercrime, information security of minors, cyberbullying, information policy, minors.