УДК 343

Горелова А.О.,
магистрант
ФГБОУВО «Российский государственный гуманитарный университет»,
РФ, г. Москва

МЕРЫ ПРОФИЛАКТИКИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В «ИНТЕРНЕТЕ», СРЕДИ НЕСОВЕРШЕННОЛЕТНИХ ЛИЦ

Аннотация: *в статье рассматриваются угрозы, которым могут быть подверждены несовершеннолетние лица в сети «Интернет». В связи со случаями престлений связанных с организацией «Синий кит» отдельное внимание уделяется привызам к сициду. Интерес автора работы также заострен на кибербуллинге, к которому часто особенно чувствительны несовершеннолетние. В статье также уделено внимание и другим аспектам, влияющим и подтвреждающим незащищенность вышеуказанных лиц, и предложены меры, которые позволяют их нивелировать, повысить юридическую грамотность.*

Ключевые слова: *криминология, киберпреступность, Интернет, несовершеннолетние, меры профилактики, сеть, информационная безопасноть.*

Resume: *The article examines the threats that minors can be exposed to on the Internet. In connection with the cases of crimes associated with the organization "Blue Whale" special attention is paid to addiction to sicide. The author's interest is also focused on cyberbullying, to which minors are often especially sensitive. The article also pays attention to other aspects influencing and confirming the vulnerability of the above persons, and suggests measures that allow them to level them, increase legal literacy.*

Key words: *criminology, cybercrime, Internet, minors, preventive measures, network, information security.*

В век информационных технологий проблема защиты прав и свобод несовершеннолетних в цифровом пространстве является одной из приоритетных и требует внимательного изучения. Какие же угрозы подстерегают несовершеннолетних в цифровом пространстве? По данным социологических исследований, детская аудитория российского Интернета насчитывает 8-10 млн пользователей до 14 лет — это около половины всех детей, проживающих в Российской Федерации. При этом около 40 % детей, регулярно посещающих Сеть, просматривают интернет-сайты с агрессивным и нелегальным контентом, подвергаются киберпресследованиям и виртуальным домогательствам.

В целом киберугрозы традиционно подразделяются на три группы: программно-технические, к которым относится умышленное распространение вирусов и троянских программ; экономические, среди которых хищение и продажа данных кредитных карт, фишинг-атаки, взломы платежных аккаунтов; контентные, связанные с возможностью публичного, в том числе анонимного, размещения в сети Интернет любых материалов, включая незаконные, пропагандирующие, например, употребление наркотиков, призывающие к терроризму, экстремизму или суициду.

Именно третья группа киберугроз представляет особую опасность для подростков, поскольку контентные киберугрозы проявляются в том числе в пропаганде употребления наркотических средств, распространении детской порнографии, материалов террористического и экстремистского характера, а также другой информации девиантной направленности.

Распространение детской порнографии посредством сети Интернет — проблема, характерная для большинства развитых стран, поэтому и меры борьбы с детской порнографией закреплены на международном

уровне. Так, Конвенция о киберпреступности предусматривает уголовную ответственность за все деяния, связанные с созданием, производством, распространением и использованием любых детских порнографических изображений[1].

Несовершеннолетние наиболее подвержены негативному влиянию извне. Иначе говоря, они обладают повышенной степенью виктимности. Поэтому проблема обеспечения информационной безопасности подростков может быть рассмотрена в двух аспектах: во-первых, как риск вовлечения несовершеннолетних в преступные сообщества посредством общения в социальных сетях; во-вторых, как риск совершения преступлений в отношении несовершеннолетних путем получения киберпреступниками персональных данных самих несовершеннолетних или их близких либо с помощью незаконного использования информационных технологий, либо в результате добровольного сообщения несовершеннолетними этих данных.

Не менее актуальной является угроза безопасности несовершеннолетних, связанная с суицидальными призывами к подросткам, осуществляемыми посредством сети Интернет. По количеству самоубийств среди несовершеннолетних в возрасте от 15 до 19 лет Российская Федерация занимает первое место в Европе и одно из первых мест в мире. При этом каждый год более 200 малолетних и около 1,5 тыс. подростков совершает самоубийство[2].

Коммуникативная активность несовершеннолетних связана с переносом определяющего влияния с родителей на ровесников. В связи с этим еще не до конца сформированная сфера ценностей и жизненных ориентиров у подростков претерпевает отрицательное и даже губительное

1 Jalil J. Combating Child Pornography in Digital Era: Is Malaysian Law Adequate to Meet the Digital Challenge? / J. Jalil // Pertanika Journal of Social Science and Humanities. — 2015. — Vol. 23. — P. 137-152

2 Брылева Е.А. Информационная безопасность несовершеннолетних как часть национальной безопасности / Е.А. Брылева // Вестник Самарского юридического института. — 2014. — № 1 (12). — С. 12-14

влияние под воздействием негативной информации, содержащейся в социальных сетях. В частности, речь идет о публичных призывах к суициду, нивелировании отношения к жизни как к главной ценности.

Следующей не менее важной угрозой информационной безопасности несовершеннолетних является кибербуллинг — психологическое насилие по отношению к ним, осуществляемое посредством сети Интернет. В отличие от традиционного буллинга (травли), все действия, унижающие подростков, производятся в виртуальном пространстве с помощью информационных и коммуникационных технологий. И буллинг, и кибербуллинг несет двойную опасность, поскольку, с одной стороны, дети подвергаются травле, что негативно сказывается на их психологическом развитии, а иногда приводит к летальным последствиям. С другой стороны , травля подростков может подтолкнуть их самих на совершение противоправных действий, что, например, по мнению многих специалистов, и произошло со студентом колледжа в Керчи, расстрелявшим своих сверстников.

Полноценное развитие индивида возможно только в определенных условиях. Большое значение имеет качество межличностного общения и психологическая безопасность в образовательной среде. Проявление психологического насилия по отношению к несовершеннолетнему накладывает на его личность существенный отпечаток[3]. Именно поэтому родителям, педагогам и психологам в школе важно своевременно выявлять подобные ситуации и пресекать их, важно проводить с детьми беседы с целью предупреждения травли. Однако если случаи буллинга еще можно выявить, поскольку они могут происходить на глазах других детей, а иногда и педагогов, то кибербуллинг выявить намного сложнее. Издевательства в Сети могут быть скрыты от посторонних глаз и быть

3 Баранов А.А. Кибербуллинг — новая форма угрозы безопасности личности подростка / А.А. Баранов, С.В. Рожи- на // Вестник Балтийского федерального университета им. И. Канта. Сер.: Филология, педагогика, психология. — 2015. — Вып. 11. — С. 62-66

известны только самому подростку, в отношении которого осуществляется травля. Именно поэтому так необходимо проводить профилактические мероприятия среди школьников, разъясняя, к каким последствиям это может привести.

Кибербуллинг представляет собой проблему международного уровня — травле в Интернете в настоящее время подвергаются подростки по всему миру. Изучение кибербуллинга следует осуществлять в контексте защиты прав несовершеннолетних, поскольку права ребенка должны пониматься широко, в том числе как право на уважительное отношение, на поддержку в обществе. Тем не менее во многих зарубежных исследованиях, посвященных кибербуллингу, вопрос о защите прав подростков отсутствует[4].

Интересен тот факт, что родители в качестве основных угроз для их несовершеннолетних детей в цифровом пространстве видят интернет-зависимость и риски, связанные с экономической и технической безопасностью[5].

Меры, направленные на защиту несовершеннолетних в сети Интернет, можно разделить на три группы: правовые, социальные и технические. Только их комплексное применение может иметь положительный результат.

К правовым мерам относится законодательное регулирование вопросов информационной безопасности несовершеннолетних. В последние годы был принят ряд законодательных актов, закрепивших законодательные меры, касающиеся информационной безопасности несовершеннолетних, и в этом направлении наметились определенные

4 Pare M. Taking Stock of Bullying and Cyberbullying Research and Introducing a Child Rights Perspective / M. Pare // United Nations Convention on the Rights of the Child: Taking Stock After 25 Years and Looking Ahead / ed. T. Liefaard, J. Sloth- Nielsen. — Boston : Brill, 2017. — P. 541-563

5 Федяй Д.С. Обращение детей и подростков к возможностям Интернета в контексте комплексной безопасности личности / Д.С. Федяй // Вестник Саратовского областного института развития образования. — 2015. — № 1. — С. 34-43

позитивные сдвиги. Так, с 2006 г. в России действует федеральный закон «Об информации, информационных технологиях и о защите информации», а в 2010 г. был принят федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию». Но при этом проблемы, связанные с созданием защищенной информационной среды, по-прежнему остаются актуальными, ведь законы зачастую не успевают за развитием информационных отношений, а законодатель не всегда может вовремя проследить ту или иную негативную тенденцию и, как следствие, не в состоянии оперативно противостоять новым рискам для подростков, появляющимся в Сети.

Проблема обеспечения информационной безопасности несовершеннолетних осложняется тем, что Интернет является глобальной информационной средой, однако применяемые юридические механизмы обычно ограничены национальными рамками. В связи с этим представляется целесообразной консолидация усилий правоохранительных органов различных стран с целью обмена ресурсами для выявления, преследования и задержания киберпреступников.

В этом аспекте интересен опыт Англии, где в 2016 г. был принят Закон о контрольных полномочиях, регламентирующий новые требования к хранению данных о поставщиках интернет- услуг, согласно которому необходимо хранить записи о подключении к Интернету в течение 12 месяцев, что обеспечивает возможность ретроспективно их исследовать.

Социальные меры, направленные на защиту прав и свобод несовершеннолетних в цифровом пространстве, должны осуществляться целым рядом субъектов: родителями, педагогами, специально созданными организациями. К социальным мерам обеспечения информационной безопасности несовершеннолетних относятся создание и внедрение программ обучения детей и подростков правилам безопасного поведения в интернет-пространстве, профилактики интернет-зависимости,

предупреждения рисков вовлечения в противоправную деятельность. Данная задача представляется актуальной прежде всего для образовательных учреждений. Большинство учебников по информатике базового уровня формирует у учащихся неполную базу личной информационной безопасности в современной информационной среде. Так, в них не рассматриваются вопросы, связанные с навыками фильтрации нежелательного контента в Интернете, противодействия деструктивным программам, фишингу, психологическим преследованиям в Сети, а также касающиеся профилактики интернет-зависимости у детей. Это может негативно повлиять на психологическое и нравственное здоровье школьников.

Правовое просвещение детей и подростков по поводу опасностей и угроз, возникающих в сети Интернет, является приоритетной задачей профилактики правонарушений в Сети. В рамках решения данной задачи в 2008 г. был создан Национальный узел интернет-безопасности в России (в настоящее время является интернет-СМИ «Центр безопасного Интернета в России»). На сайте Центра действует горячая линия, на которую дети и подростки могут сообщить о противоправном контенте, а также линия помощи жертвам интернет-угроз.

В рамках проекта «Дети онлайн» разработаны материалы, посвященные безопасному поведению в Интернете. На сайте фонда «Дружественный Рунет» доступны рекомендации для детей, родителей и педагогов по предотвращению рисков, связанных с использованием несовершеннолетними сети Интернет.

Еще одной социальной мерой профилактики киберугроз для подростков является проведение единых уроков безопасности школьников в сети Интернет. Единый урок, впервые проведенный в 2014 г., а в 2016 г. прошедший более чем в 36 тыс. школ и в 350 библиотеках России, — это результат совместных усилий государства, общества и представителей IT-

отрасли, направленных на то, чтобы сделать интернет- пространство безопасным для подростков[6].

С 2012 г. Координационным центром национальных доменов .RU и .РФ при поддержке ПАО «Ростелеком» реализуется социально-образовательный проект для школьников «Изучи Интернет — управляй им ». Проект позволяет подросткам получить базовые знания об устройстве сети Интернет. Цель проекта заключается в повышении уровня цифровой грамотности несовершеннолетних пользователей Интернета в современной интерактивной форме.

Несмотря на ряд предпринимаемых мер, следует констатировать, что российские школьники пока в должной степени не вовлечены в просветительский процесс, направленный на обучение информационной безопасности в сети Интернет на постоянной основе. На уроках информатики не проводится каких-либо специальных мероприятий, посвященных информационной безопасности. В рамках иных школьных предметов такое обучение также отсутствует. Тема информационной безопасности, включая защиту от кибербуллинга, может затрагиваться в рамках классных часов, при этом данные занятия не носят системный характер, а проходят в связи с возникновением какой-либо ситуации в классе, школе, городе или стране. Причем учителя, которые проводят такие занятия, как правило, сами не владеют достаточным уровнем правовых и информационных знаний, необходимым для ознакомления детей с темой. Следует констатировать, что многие современные подростки в сфере информационных технологий, включая информационную безопасность, знают много больше своих учителей информатики.

Выходов из сложившейся ситуации может быть несколько. В первую очередь необходимо проводить курсы повышения квалификации для

6 Дети в информационном обществе. 2017.

самих учителей, повышая их уровень знаний и умений в сфере информационной безопасности в сети Интернет. Такие курсы могут проходить как в традиционной форме, так и онлайн. Сейчас их предлагается достаточно много.

Одним из способов повышения правовой и информационной грамотности детей в сфере информационной безопасности может стать проведение занятий по правовому просвещению, по информационной гигиене. Такие занятия могут организовывать, например, юридические клиники вузов в рамках программ правового просвещения. Так, Центр бесплатной правовой помощи (юридическая клиника) Волгоградского института управления — филиала РАНХиГС на регулярной основе проводит такие занятия на базе школ для учеников разных классов, а также на базе Волгоградской областной библиотеки для молодежи. В рамках занятий школьникам рассказывается о юридически грамотном поведении в сети Интернет, о необходимости соблюдения этических норм в киберпространстве, правовых последствиях кибербуллинга, иных форм нарушений, дети получают знания об информационной безопасности с точки зрения раскрытия персональных данных и пр. Несмотря на то что интернет-среда для подростков становится обычной, многие из них не задумываются о последствиях своих действий в Интернете. Очень важно, чтобы подобные занятия проводились не только в форме лекций, но и в практической форме, чтобы несовершеннолетние могли получить необходимые им навыки.

Повышение уровня технической грамотности детей и подростков и проведение соответствующих занятий могли бы взять на себя студенты технических вузов в рамках осуществления волонтерской деятельности.

Технические меры обеспечения защиты прав и свобод несовершеннолетних в сети Интернет имеют свою специфику. Борьба с некорректным поведением в цифровом пространстве (кибербуллинг,

клевета, распространение персональных сведений) ведется по двум направлениям. В первую очередь это развитие технических приспособлений, ограничивающих нежелательный контент (настраиваемые пользователями фильтры, использование цензуры), возможность пожаловаться на оскорбительное поведение в социальных сетях и на веб-сайтах администрации данного ресурса (так называемые кнопки тревоги), а также возможность установить настройки конфиденциальности персональных аккаунтов. С другой стороны, осуществляется обучение пользователей Интернета основным правилам безопасности и корректного поведения по отношению к другим пользователям.

Следует отметить, что названные выше способы не могут в полной мере защитить пользователей от некорректного поведения в цифровом пространстве. Нередки случаи, когда администрация ресурса применяет меры взыскания к нарушителям несвоевременно либо не реагирует на жалобы пользователей вовсе. Что касается самих нарушителей, они могут вместо заблокированных по жалобам других пользователей аккаунтов создавать новые, вымышленные, и продолжать свои действия против жертвы.

В последнее время в различных странах получила распространение обширная анонимная сеть — так называемая Deep Web («Глубокая паутина»), представляющая собой группу сайтов, которые находятся в зашифрованном сетевом пространстве и поэтому не могут быть обнаружены традиционными поисковыми механизмами. Основная цель анонимных вебсайтов — хранить не предназначенную для широкой общественности информацию, часто используемую для преступной деятельности, связанной с торговлей наркотиками, мошенничеством в финансовой сфере, незаконным оборотом оружия, шпионажем, сексуальным надругательством над несовершеннолетними. Анонимные

веб-сайты могут быть также использованы в преступных целях. Например, известны случаи онлайн-продажи наркотиков через анонимный сайт Silk Road. При этом данные сайты не в состоянии гарантировать полную защиту от хакерских атак.

Таким образом, в настоящее время существует ряд правовых, социальных и технических мер, призванных обеспечивать информационную безопасность несовершеннолетних. Тем не менее следует констатировать их недостаточную эффективность в связи с отсутствием комплексного подхода, слаженной деятельности уполномоченных субъектов. С другой стороны, сама сфера защиты подростков от негативного воздействия в цифровом пространстве быстро меняется, обрастает все новыми угрозами со стороны киберпреступников.

Проблема защиты несовершеннолетних в цифровом пространстве является комплексной, поскольку для ее успешного решения необходима консолидация усилий целого ряда субъектов в лице как уполномоченных органов и учреждений, так и общественных объединений и граждан.

Использованные источники:

1. Брылева Е.А. Информационная безопасность несовершеннолетних как часть национальной безопасности / Е.А. Брылева // Вестник Самарского юридического института. — 2014. — № 1 (12). — С. 12-14.

2. Баранов А.А. Кибербуллинг — новая форма угрозы безопасности личности подростка / А.А. Баранов, С.В. Рожи- на // Вестник Балтийского федерального университета им. И. Канта. Сер.: Филология, педагогика, психология. — 2015. — Вып. 11. — С. 62-66.

3. Федяй Д.С. Обращение детей и подростков к возможностям Интернета в контексте комплексной безопасности личности / Д.С. Федяй //

Вестник Саратовского областного института развития образования. — 2015. — № 1. — С. 34-43.

4. Jalil J. Combating Child Pornography in Digital Era: Is Malaysian Law Adequate to Meet the Digital Challenge? / J. Jalil // Pertanika Journal of Social Science and Humanities. — 2015. — Vol. 23. — P. 137-152.

5. Pare M. Taking Stock of Bullying and Cyberbullying Research and Introducing a Child Rights Perspective / M. Pare // United Nations Convention on the Rights of the Child: Taking Stock After 25 Years and Looking Ahead / ed. T. Liefaard, J. Sloth- Nielsen. — Boston : Brill, 2017. — P. 541-563.