

6. Савина Н. Н. Концепция преодоления делинквентности / девиантности средствами креативной педагогики // Академический журнал Западной Сибири. 2011. № 1. С. 19–20.

7. Федеральный закон «О полиции» от 07.02.2011 № 3-ФЗ // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_110165/.

УДК 379.8.092.3-053.2:004.738.5.056

С. В. Ченушкина

S. V. Chenushkina

*ФГАОУ ВО «Российский государственный профессионально-педагогический университет», Екатеринбург
Russian state vocational pedagogical university, Ekaterinburg
svch2003@yandex.ru*

КИБЕРБЕЗОПАСНОСТЬ ДЕТЕЙ В ЦИФРОВОМ ПРОСТРАНСТВЕ CYBERSECURITY OF CHILDREN IN THE DIGITAL SPACE

Аннотация. В статье рассматриваются риски, возникающие у детей в цифровом пространстве, приведены виды, возникающих киберугроз: кибербуллинг, кибермошеничество, буллицид и др. рассматриваются разные способы позволяющие снизить риски пребывания в среде Интернет.

Abstract. The article discusses the risks that arise in children in the digital space, the types of emerging cyber threats are given: cyberbullying, cyberbullying, bullying, etc. various ways are considered to reduce the risks of being in the Internet environment

Ключевые слова: кибербезопасность, дети, подростки, Интернет, угрозы, цифровое пространство, кибербуллинг, кибермошеничество, буллицид

Keywords: cybersecurity, children, teenagers, Internet, threats, digital space, cyberbullying, cyberbullying, bullying

По данным национального центра статистики образования, 94 % детей в возрасте от 3 до 18 лет имеют доступ в сеть Интернет, т. е. являются активными участниками цифрового пространства, создаваемого разными устройствами: мобильные телефоны, планшеты, компьютеры, игровые консоли и принимающие разные формы: сайты, социальные сети, игры или мессенджеры. Среднее время, проведенное практически бесконтрольно в сети в сутки от 7 до 14 часов, увеличилось в период пандемии. Более 80 процентов имеют профиль в социальных сетях.

Один из вариантов определения, чем занимается ребенок в сети, постоянное подглядывание в экраны его устройств, что физически невозможно, как и порой понять – проводится ли учебное занятие в игровой форме

или это действительно компьютерная игра. По опросу детской аудитории стало понятно, что для мальчиков главным времяпрепровождением являются компьютерные игры, а для девочек – более важно общение, поэтому и заботиться о них нужно соответственно.

Единственным способом ограждения ребенка от зависимости и возможных угроз цифрового пространства – это или полностью ограничить доступ к сети, или контролировать и фильтровать поток информации в новостных лентах, сайтах и интернет-общениях, что, конечно, вызывает большое количество споров и конфликтов между взрослыми и детьми, расценивающих такие действия как попытки ограничения своей свободы.

Рассмотрим два ключевых понятия: *киберпреступность* – это преступная деятельность, в рамках которой используются либо атакуется компьютер, компьютерная сеть или пользователь; и *кибербезопасность* – это совокупность методов защиты от атак злоумышленников. Большинство кибератак совершается с целью получения финансовой прибыли, но могут быть личные или политические мотивы [3].

Освящением проблемы и привлечением населения России к проблеме кибербезопасности в последние годы начали заниматься многие государственные организации и частные фирмы. Российская электронная школа в рамках проекта «Кибербезопасность для детей и взрослых» сняла серию видеороликов по основным киберугрозам в сети: «На игре», «Максимальный репост», «Виртуальная реальность», «Ты не один», «Калькулятор», «Лучший подарок» [1].

Киберпреступники часто нацелены на детей, подростков и пожилых людей, они более одинокие и доверчивые, менее опытные в киберпространстве, что и используют кибермошенники. Финансовые схемы не отличаются сложностью и часто используют доверие детей к взрослым, представителям финансовой сферы или работникам правоохранительных органов; по телефону нет возможности проверить документы или зачастую ставятся такие условия, при которых нужно быстро принимать решение: «Твой папа попал в беду», «Мамину карточку пытаются взломать»... Возможность покупки гаджетов, атрибутики для персонажа онлайн игры, «донаты» или дополнительный заработок, также могут привлечь внимание подростка, воспользовавшись данными банковской карты родителей или молодежной карты для приобретения.

Основной риск здесь – утечка персональных данных, денежных средств или шантаж. Ограничение денежных средств, уделение внимания развитию финансовой грамотности, правилам поведения с конфиденциальной информацией, сложные пароли и внимательность к элементам сайта – помогут решить

проблему. У любой банковской карты, есть возможность установления ограничения на лимиты покупок в сутки и сумм онлайн-платежей.

Компьютерные игры не сдают свои позиции. Игровая зависимость приобрела масштаб эпидемии, онлайн-игры становятся доминантной в жизни ребенка. Базовые ценности и получение образования, которые в момент взросления только занимают свои ниши, «проигрывают» в динамичности и значимости жизни в виртуальном мире, зачастую главным элементом которого становятся компьютерные «убийства» и обесценивание человеческой жизни.

К этой же серии относится и интернет-зависимость – желание находится в Интернете как можно больше: компьютерное общение, просмотр ленты социальных сетей, видеороликов, информация поступает порционно, разнообразного содержания, что не наскучивает ребенку, эмоции становятся более яркими при получении виртуальных призов, лайков в социальных сетях.

Подобные зависимости относят к психологическим патологиям или замещению решения реальных проблем: при стрессах (смерти близких, разводы, ссоры в семье), необходимости самоутверждения, отсутствию внимания близких и друзей, статуса в классе и др. Наиболее эффективным станет ограничение цифровых возможностей «игрока» (покупок, ограничение тарифов) и когнитивно-поведенческая терапия для изменения мышления ребенка и переориентирование интересов.

При общении в Интернете ребенок, как и любой участник общения, может стать кем угодно, прикрываясь маской, фотографиями и манерой общения. Аккаунты социальных сетей или сводятся к «черному квадрату» в профиле, или к собственной пиар-кампании – фотографий, видеороликов и отмеченных меток мест, что делает подростка уязвимым для кибергруминга, при котором дети становятся объектами преступлений лиц, посягающих на половую неприкосновенность, членов сект или интернет-аферистов, выманивающих личную информацию и ставящие их в материальную или иную зависимость.

В цифровом пространстве все стороны человеческой личности проявляются гипертрофированно, информация передается между членами цифрового сообщества мгновенно, эквивалентом положительных эмоций становятся лайки, смайлы, открытки, эквивалентом отрицательных – дизлайки, хейт и кибербуллинг. Травля в сети может идти за спиной самого участника, фразы, произносимые при живом общении, легко пишутся с использованием клавиатуры. Основные виды кибербуллинга и способы защиты, были рассмотрены в статье «Защита прав ребенка от кибербуллинга в образовательной организации» [2].

Следующим шагом слома личности ребенка и худшим вариантом направления несформированной психики, как следствий буллинга, кибербуллинга, решения личных проблем, становится буллицид – доведение до суицида. Интернет-сообщества данной тематики появились еще в 2011–2013 гг., одни из них, например, как первичный «Синий кит», были объединением пользователей, обсуждающих личные проблемы, которые развились в киберигру с набором заданий, последнее из которых станет, – совершение суицида. В игре есть кураторы, которые диктуют свои правила игры: всегда одно и то же время встреч (поздняя ночь), первое задание для всех одно – «написать лезвием на руке «Синий Кит», дальше задания все изощреннее. Школьники приходят в школы с порезами, в депрессии могут рисовать или печатать изображения бабочек, китов, единорогов, медуз, кошек.

Надзорные органы и владельцы социальных сетей пытаются контролировать и отслеживать в интернете «групп смерти» по поиску слов и картинок, но аккаунтов все больше, кураторы скрываются. К их поиску присоединились «дельфины» – добровольцы из числа подростков, родителей пострадавших детей или профессиональных психологов, пытающихся отговорить детей.

Необходимо обращать внимание на закрытость ребенка, профили в социальной сети, демонстративные жесты и закрытие лиц на фотографиях, фото с высоты, черные одежды и худоба, отказ от повседневных дел и склонность к прослушиванию депрессивной музыки, цитирование стихотворений, посвященные смерти, например, Сергея Есенина или Иосифа Бродского.

Анализ профиля, просмотр поисковых запросов и истории посещения браузера, помогут сузить и рассказать об увлечениях ребенка, подписок и групп по интересам. Необходимо также обращать внимание на маркировку контента по возрастной категории (0+, 6+, 12+, 16+, 18+) и использование специальных приложений и программ, показывающих статистику просмотров и геолокации детей, например, «KasperskySafe Kids» от фирмы «Kaspersky».

Оградить ребенка от угроз цифрового пространства невозможно как невозможно на 100 % гарантировать безопасность в Интернете. Психическая устойчивость, просвещение в вопросах кибербезопасности и поведения в сети Интернет, уважение к базовым ценностям, помогут уберечь ребенка. Не забывайте, что «цифровой двойник» вашего ребенка, является отражением его реальной личности, только в искаженном варианте отдельных черт и потребностей, описанных А. Маслоу (исключая физиологические).

Список литературы

1. Проект «Кибербезопасность для детей и взрослых» Российской электронной школы. URL: <https://resh.edu.ru/page/cyber-project>.

2. Ченушкина С. В. Защита прав ребенка от кибербуллинга в образовательной организации // 30 лет конвенции о правах ребенка: современные вызовы и пути решения проблем в сфере защиты прав детей: сборник материалов Международной научно-практической конференции, Екатеринбург, 17 ноября 2020 г. Екатеринбург: Рос. гос. проф.-пед. ун-т, 2020. С. 282–286. URL: <https://elar.rsvpu.ru/handle/123456789/32891>.

3. Что такое киберпреступность? Защита от киберпреступности // Сайт «Kaspersky». URL: <https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime>.