УДК 004.056.5

БЕЗОПАСНОСТЬ ДЕТЕЙ В СЕТИ ИНТЕРНЕТ

Шляхтич П. С. 1

1 Саратовский Государственный медицинский университет имени В.И. Разумовского, Саратов, e-mail: polinashliahtich5@gmail.com

В этой статье рассмотрены наиболее эффективные пути и методы по вопросам безопасности детей младшего и среднего школьного возраста. Проведено анкетирование по вопросам, связанным с безопасностью детей от влияния нежелательного контента, киберагрессии, интернет-мошенничества, обеспечить информационную безопасность детей и подростков в сети интернет.

Ключевые слова: Кибербуллинг, контент, интернет-афера, флейминг, хиплейпинг, фишинг, киберугроза.

INTERNET SAFETY FOR CHILDREN

Shliahtich P. S. 1

1 Saratov State Medical University named after V. I. Razumovsky, Saratov, e-mail: polinashliahtich5@gmail.com

Keywords: cyberbulling, content, internet-scram, flaming, hippleping, phishing, cyberthreat.

In this article, we will look at the most effective ways and methods for the safety of children of primary and secondary school age. You will find information on how to: protect children from the influence of inappropriate content, cyber aggression, Internet fraud, ensure the information security of children and teenagers online. This article will be useful for parents, people who are trying to protect children from everything that causes them discomfort.

Введение. Безопасность детей в сети на сегодняшний день очень актуальная тема, так как нынешнее поколение людей не только взрослые, но и дети проводят много времени в виртуальной реальности. Сегодня

информационные средства, прежде всего телевидение, интернет не только выполняют свои прямые функции по информированию населения, но и формируют взгляды, вкусы, не только людей, но и детей. Дети очень любознательные они хотят познавать много нового, учиться, им все интересно, но на этом пути их могут ожидать разного рода опасности, которые надо обходить стороной, конечно не без помощи родителей, людей, которые всегда поддержат и подскажут правильный путь. В современном мире человек уже не представляет жизни без телефона, ноутбука и, конечно же, интернета. Прогресс техники охватил большую часть нашего жизненного пространства. Мы сами порой не замечаем, сколько времени проводим в интернете, подавая пример своим детям, младшим братьям или сестрам. Ребенок – это формирующаяся личность, которая перенимает модели поведения с родителей, старших детей. Влияние интернета является одним из факторов формирования психологического развития ребенка и его мировосприятия. У интернета, безусловно, много положительных сторон, но также есть и отрицательные. Чем же опасен интернет для ребенка [1]?

Цель исследования. Выявить знания у подростов, посвященные вопросам безопасности в интернете.

Материал и метод исследования. Для достижения поставленной цели была разработана специальная анонимная анкета, которую школьники старших классов самостоятельно заполняли. В исследовании приняли 20 подростков-старшеклассников, в возрасте 16-17 лет. Из них девушек было 10 человек, мальчиков 10 человек. Анкета заполнялась на бумажном носителе в условиях школы. Перед исследованием было разъяснены цели и задачи исследования и получено согласие на участие. Исследование сплошное, подготовки к исследованию не осуществлялось.

Результаты исследования и их обсуждение. Информационные технологии все больше проникают в общественные сферы, что вызывает значительный рост разного рода киберугроз и приводит к серьезным изменениям в сознании миллиардов людей. Киберугрозы – это угрозы информационной

безопасности. В связи с тем, что данный вопрос имеет большое социальное значение, в анкету был включен данный вопрос. Как показало исследование, на вопрос, связанный со знанием данного вопроса, все опрошенные дали положительный ответ. Из этого можно сделать заключение, что все опрошенные, не зависимо от пола, ориентированы в данном вопросе.

Вирусы – скрытно проникают в компьютерные системы. На вопрос связанный со знанием, что такое компьютерный вирус, какую угрозу он представляет и способы защиты от него, все 100% опрошенных отметили, что им известны данные угрозы и способы защиты от него.

Спам не только вызывает раздражение у пользователей, но и забивает каналы связи, расходует трафик, отвлекает от работы. Как показал опрос, все 100% опрошенных ответили, что знают, что такое спам и какие угрозы он несет.

Фишинг, в отличие от спама, нацелен на узкие группы пользователей и содержит сообщения с социальным контекстом, призывающие потенциальную жертву открыть исполняемый файл или перейти на сайт. Результаты, полученные при ответе на знания по этому вопросу, отражены на рисунке 1.

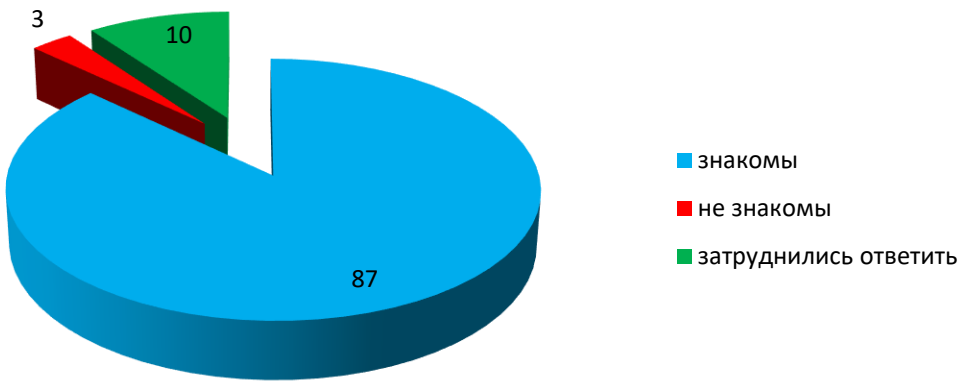

Рисунок 1. Результаты ответов на вопрос связанный со знанием фишинга (в %)

Как видно из данных, которые отражены на рисунке 1, большинство опрошенных – 87% знают, что такое фишинг, вместе с тем, 3% ответили отрицательно и еще 10% опрошенных затруднились ответить.

Нежелательный контент: стандартный набор: суициды, сцены насилия, жестокости, порнография. Бывает и нестандартный “нежелательный контент” – Кибербуллинг, одна из самых распространённых угроз, связанных с общением в Сети. Это форма коллективной травли детей с помощью телефонов и Интернета. Кибербуллинг опасен не меньше, чем издевательства в привычном понимании, ведь жертва кибербуллинга находится в большом психологическом напряжении, и не каждый ребёнок сможет его вынести самостоятельно. И конечно дети не хотят рассказывать об этом родителям, а в одиночку справиться с этим очень непросто. Кибербуллинг включает в себя: анонимные угрозы — пересылка писем без подписи отправителя, содержащих угрозы, оскорбления, часто с использованием ненормативной лексики; преследование — рассылка неприятных писем своей жертве продолжительное время, которая в дальнейшем может вылиться в шантаж какими-либо фактами её жизни; использование личной информации — взлом электронной почты или страниц в социальных сетях для получения личной информации для шантажа или издевательств.

Как показывает проведенный опрос, больше половины респондентов – 65% знают, что такое кибербуллинг, однако достаточно большой процент опрошенных – 30% ответили, что не знают, что это такое, а 5% затруднились ответить на данный вопрос. Результаты ответов на вопрос, считаете ли Вы, что кибербуллинг представляет реальную угрозу, отражены на рисунке 2.

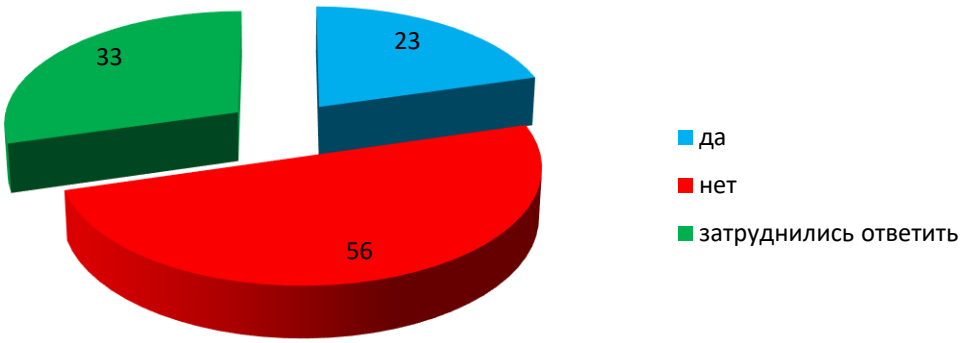

Рисунок 2. Результаты ответов на вопрос, считаете ли Вы, что кибербуллинг представляет реальную угрозу (в %)

Как можно увидеть, были получены достаточно интересные ответы на данный вопрос. Это связано с тем, что больше половины опрошенных – 56% считают, что кибербуллинг не представляет угрозу, при этом только 23% опрошенных отметили, что он представляет из себя реальную угрозу, а 33% затруднились дать ответ. Исходя из этого можно сделать заключение, что данный вид можно отнести к реальной угрозе, при этом больше половины подростков не считают его угрозой, что может нанести колоссальный вред. При ответе на вопрос, связанный с тем, приходилось ли сталкиваться с данной угрозой, 45% опрошенных ответили положительно, 35% отрицательно, а 20% затруднились дать ответ.

Разновидностью кибербуллинга является **флейминг** — обмен эмоциональными репликами между агрессором (иногда их может быть несколько) и жертвой с целью получения удовольствия от нанесения оскорблений. Как показали наши исследования, что это такое знают 86% опрошенных, не знают – 10%, затруднились ответить 4%. При этом, при ответе

на вопрос, считаете ли Вы, что флейминг является неприемлемой формой общения и несет в себе потенциальные угрозы, положительно ответили 76%, отрицательно – 30%, затруднились ответить – 10%.

Хипплейпинг — видеозаписи с издевательствами, которые «заливают» на ресурсы, где их сможет увидеть большое количество пользователей. Такие ролики, естественно, «заливаются» без согласия потенциальной жертвы. На вопрос знаете ли Вы, что такое хипплейпинг, положительно ответили 85% опрошенных, 5% ответили отрицательно, 10% - затруднились дать ответ. При этом 85% считают, что хипплейпинг, нельзя отнести к реальной угрозе, а 15% ответили, что это реальная угроза. Однако, по результатам опроса, с такими действиями столкнулись лишь 8% респондентов, а 92% опрошенных не сталкивались с данным явлением, возможно именно этим можно объяснить столь высокий процент ответов, которые считают, что данные действия не являются угрозой.

Другая проблема, которая таит в себе виртуальное общение – это разговоры с незнакомцами. Дети легче поддаются убеждению, они более доверчивы, поэтому могут совершенно спокойно рассказать своему новому виртуальному другу то, что в обычной жизни никогда бы не рассказали. Незнакомцы входят в доверие к ребенку и узнают необходимую им информацию: номера банковских карт или день, когда вся семья уедет в отпуск, оставив надолго пустую квартиру. Общение с незнакомцами в сети может перерасти в реальное общение в жизни, такие свидания очень опасны, так как злоумышленники именно через социальные сети выискивают и выманивают своих жертв. На вопрос, считаете ли Вы, что общение с незнакомцами несет в себе потенциальную угрозу, 56% респондентов ответили положительно, в тоже время, достаточно большой процент опрошенных – 32% ответили, что не считают такое общение несущим угрозы, 12% опрошенных затруднились дать ответ. Исходя из полученных результатов можно сделать заключение, что

необходимо уделять большее внимание данному вопросу, как со стороны родителей, так и со стороны школьных учителей.

Заключение: виртуальный мир, сегодня является местом, где человек проводит все больше и больше времени, это быстро, удобно, но следует помнить, что интернетом надо пользоваться с пользой для себя, а не во вред своему эмоциональному и физическому здоровью. Детям надо осваивать интернет вместе с родителями, так как интернет – это не только огромное количество возможностей, но и великое множество подстерегающих опасностей для начинающего маленького пользователя, поэтому детям и особенно родителям надо использовать всевозможные пути по обеспечению безопасности. [1,2,3]

Список использованных источников

1) Поляков В.В., Кузнецов М.И., Марков В.В., Латчук В.Н. Основы безопасности жизнедеятельности 5 класс: учебник. – М.: ДРОФА, 2019.

2) Вангородский С.Н. Основы кибербезопасности. 5–11 классы: учебно-методическое пособие. – М.: ДРОФА, 2019

3) Учебные материалы Региональной общественной организации «Центр интернет-технологий» (РОЦИТ),1996–2019.