Проблема безопасности детей в сети интернет: методика обучения информатике в базовом курсе

Карпов А.А.[1], Векслер В.А.[2]
[1]start6456@gmail.com, [2]vitalv7486@gmail.com
Саратовский государственный университет имени Н.Г.Чернышевского

Ключевые слова: методика, безопасность в интернете, информационные технологии, интернет.

Использование сети интернет подрастающим поколением является одним из важных показателей уровня развития информационного общества. На данный момент сложно представить, что какая-либо область деятельности будет обходиться без использования ИКТ, особенно это касается детей. В процессе своего обучения современные школьники вовсю используют интернет, чтобы подготовить доклад, найти статьи научных деятелей и дополнительную литературу. Привыкшие к безграничным возможностям современных технологий, они зачастую не могут разглядеть рисков и угроз и в результате оказываются среди наиболее уязвимых ее пользователей, сталкиваясь с мошенниками, преступниками и материалами, которые не подходят для их возрастной группы.

Прежде всего, информационная безопасность детей - это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию. [1] Основные опасности в Интернете для детей и подростков следующие:

1. Кибербуллинг.
2. Использование Интернета для манипуляции сознанием детей и подростков.
3. Незнакомцы в социальных сетях.
4. Кибермошенничество.
5. Просмотр сайтов для взрослых.

Кибербуллинг

Кибербуллинг – это травля пользователя через все каналы сетевого общения: социальные сети, форумы, чаты, мессенджеры. Проводить кибербуллинг могут как одноклассники, интернет-друзья и т.д., так и совершенно посторонние люди. Интернет-травля может принимать разные формы: оскорбления через личные сообщения, публикация и распространение конфиденциальной, провокационной информации о жертве. В интернете, как правило, ребенок находится один на один с потенциальным обидчиком, который к тому же уверен в своей анонимности и может действовать более нагло.

По мнению эксперта «Лаборатории Касперского» [2], борьба с кибертравлей технически не так проста, поэтому и программный родительский контроль не столь эффективен. При этом дети не способны справиться с агрессорами в одиночку, но зачастую не обращаются за помощью к взрослым, будучи

запуганными угрозами, либо просто из-за отсутствия доверия к близким людям. Поэтому самую важную роль в защите ребенка от кибер-террора играют отношения с родителями.

Использование интернета для манипуляции сознанием детей и подростков

На неокрепшее детское сознание также могут оказать влияние различные группы-секты, которые встречаются как в социальных сетях, так и на просторах сети в целом. Так же, как и в случае с кибербуллингом, своевременное вмешательство родителей, а также специальная программа контроля, ограничивают посещение ребенком незнакомых сайтов.

Незнакомцы в социальных сетях

Ребенок может передать незнакомцам свои персональные данные, поделиться номером кредитки мамы, может сфотографировать квартиру, сообщить адрес, показать интерьер и ценные вещи, рассказать, что семья уезжает в отпуск, и т.д. Нужна очень серьезная кооперация всей семьи, чтобы уяснить: все, что мы выкладываем в интернет, становится достоянием огромного круга людей, которые далеко не всегда дружелюбно настроены.

Кибермошенничество

Для кражи личной информации пользователя, применяются все более сложные фишинговые схемы, в том числе с использованием узнаваемых брендов, способные обмануть даже взрослого человека. Таким образом ваши личные данные могут оказаться в открытом доступе. Так, в мае 2014 года Роскомнадзор выявил более 200 сайтов, распространяющих в открытом доступе персональные данные несовершеннолетних россиян и их родителей.

Просмотр сайтов для взрослых

Согласно исследованиям[3] из всех сайтов с маркировкой 18+ наибольший интерес для российских детей представляют эротические и порнографические сайты – 46,4%, на втором месте оружейная тематика – 26,4%, на третьем – нецензурная лексика – 10,7%.

Следует обратить внимание, что указанные проценты - это удельный вес не всех посещаемых несовершеннолетними сайтов, а только входящих в категорию нежелательных. Ещё точнее – в эти проценты вошли и неудачные попытки попасть на «взрослые» сайты, если они были заблокированы модулем «Родительский контроль». Вывод этого исследования очевиден, безопасность ребенка в сети осуществляется строгим контролем со стороны родителей.

Информационная безопасность обучающихся в школе

Помимо родительского контроля, образовательное учреждение обязано обеспечить безопасность ребенка от интернет-угроз. Информационная безопасность обучающихся в школе может быть достигнута за счет успешной реализации педагогических условий (наличия уголков безопасности в каждом кабинете с установленными компьютерами; утвержденных режимов работы кабинетов образовательного учреждения с установленными компьютерами; проведения инструктажей безопасности при работе в Интернет; обеспечением мотивированного включения подростков в разнообразные виды деятельности в информационной сфере). Учитель должен иметь представление о

классических средствах защиты информации, таких как физические средства (механические, электрические, электромеханические, устройства и системы), аппаратные средства (электронные и электронно-механические устройства, встраиваемые в аппаратуру системы обработки данных), программные средства (специальные пакеты программ или отдельные программы), организационные средства (организационно-технические мероприятия, специально предусматриваемые в технологии функционирования системы с целью решения задач защиты информации), законодательные средства (нормативно-правовые акты, с помощью которых регламентируются права и обязанности, а также устанавливается ответственность), психологические (морально-этические средства, нормы и этические правила).

Список литературы

[1] Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

[2] «Лаборатория Касперского» Умный контроль для умных детей. [Электронный ресурс] - режим доступа: https://www.kaspersky.ru/blog/smarter-safe-kids/22917/

[3] «Лаборатория Касперского» Дети в Сети: формула безопасности. [Электронный ресурс] - режим доступа: https://securelist.ru/deti-v-seti-formula-bezopasnosti/20171/