Информационная безопасность младших школьников

Информационная безопасностью детей называют состояние защищённости, при котором отсутствуют какие-либо риски, связанные с причинением вреда через какую-либо информацию, в большинстве случаем распространяемая в Интернете, несущая вред психологическому, духовному, физическому и нравственному развитию.

Интернет – это огромная «паутина информации» и ребёнок младших классов, захваченный огромными возможностями современных технологий, зачастую не может разглядеть рисков и угроз сети и в результате оказывается одним из самых уязвимых пользователей. Сталкиваясь с угрозами при «неумелом» использовании интернета, стоит выделить четыре вида рисков:

∙**Контентные риски** **–** эти риски связанны с распространением различных материалов, таких как картинок, гифок, текстов, аудио/видео файлов или ссылок, имеющие противозаконную, вредоносную, порнографическую информацию, возможно, разжигающую расовую ненависть, призыву к чему-либо, пропаганду азартных игр, наркотических веществ, суицида.

Столкнуться с таким видом рисков можно практически везде: будь то социальные сети, видеохостинги, сайты, блоги.

∙**Электронные** (или же программные) **риски** **–** это риски, связанные с кражей вашей персональной информации, будь то личные фотографии, пароли, данные от кошельков, банковских счетов или карт, или же атакой вредоносных программ. Вредоносные программы – это «хакерское» программное обеспечение, задачей которой является нанесение вреда вашему компьютеру и хищением личной информации, простым языком такие команды называют: «вирусы», «черви», «трояны», «ратники», «боты» и так далее. Они часто встречаются на вредоносных сайтах или в подозрительных ссылках.

∙**Коммуникационные риски –** это вид рисков, связанный с коммуникацией и межличностным отношениями различных интернет-пользователей. Примерами таких угроз могут быть кибербуллинг, незаконные контакты, знакомства в сети и встречи с интернет-знакомыми в реальной жизни. С этом видом рисков можно столкнуться при общении в чатах, мессенджерах, социальных сетях, сайтах знакомств, форумах или блогах.

∙**Потребительские риски –** это вид угрозы, включающий в себя злоупотребление в интернете правами потребителя. К ним относятся риск приобретения товара низкого качества, различные подделки, контрафактную и фальсифицированную продукцию, потерю денежных средств без приобретения товара или услуги, хищение персональной информации с целью мошенничества. Часто можно встретить на онлайн-маркетплейсах, таких как «Вайлдберриз» или «Алиэкспресс»

По результатам исследования «Дети России онлайн», проведенного в 11 регионах Российской Федерации сотрудниками Фонда Развития Интернет и факультета психологии МГУ имени М.В. Ломоносова проведённом в 2011 году, можно узнать о том, что школьники начинают выходить в сеть и активно пользоваться всеми интернет-ресурсами от девяти до десяти лет, среди которых 70 % не имеют какого-либо контроля.

Почти каждый третий школьник, возраст которого от девяти до десяти лет использует для выхода в сеть мобильный телефон. Каждый второй ребенок выходит в сеть ежедневно, и почти треть – один или два раза в неделю. Более четверти опрошенных детей находятся онлайн от 7 до 14 часов в неделю (это около одного-двух часов в день), каждый шестой ребенок - от 14 до 21 часа, а каждый пятый – более 21 час. Основной деятельностью детей в интернете стало общение. Так, более 75% российских детей указали, что у них есть профиль в социальной сети, а почти треть имеет больше одного профиля в разных сетях. У третьей части опрошенных детей профили открыты и доступны всем пользователям. От 60 до 80% российских школьников выкладывают в сети фамилию, точный возраст, номер школы. Дети в возрасте 9-10 лет имеют больше 10 друзей в социальных сетях, у 32% больше 50 друзей. При этом половина российских детей от 9 до 16 лет постоянно знакомится в интернете с новыми людьми, а каждый пятый признается, что встречался с интернет-знакомыми в реальной жизни. В то же время как каждый второй ребенок 9-16 лет считает, что в интернете есть что-то плохое для его сверстников, а каждый пятый хотя бы раз сталкивался в интернете с чем-либо, что огорчило или обеспокоило его.

Интернет имеет огромное количество угроз, с которыми может столкнуться почти каждый школьник младших классов, поэтому, по моему мнению, эти способы станут самыми эффективными и быстро действенными:

∙Образовательная программа в школе (разработка полноценного урока и проведение тренингов для учителей и родителей, организация тематических классных часов и родительских собраний)

∙Программные средства защиты (Внедрение родительского контроля на гаджетах учащихся, настройка фильтров и блокировка вредоносного контента с учётом возрастных ограничений учащихся)

∙Психологическая поддержка (Организация консультаций со школьным психологом для детей и родителей, разработка методики раннего выявления и предотвращения кибербуллинга на раннем этапе)

По мнению большинства исследователей в области компьютерной безопасности, эти методы борьбы повышают уровень информативности младших школьников в вопросах кибербезопасности, снижение количества случаев кибербуллинга и других угроз в интернете среди учащихся младших классов, формирование у детей навыков критического восприятия информации.

Информационная безопасность школьников младших классов – это важный аспект современного образования, требующий внимания со стороны учителей, родителей и общества в целом. Осведомлённость детей об угрозах в интернете и способах защиты от них является ключевым элементом их общего развития и безопасности.

Необходимо воспитывать у детей навыки критического мышления и ответственного поведения в сети, а также обеспечивать их поддержку и защиту со стороны взрослых. Совместные усилия всех заинтересованных сторон способны создать безопасную и поддерживающую среду, в которой каждый ребёнок сможет безопасно «исследовать» мир информационных технологий.