«Деятельность вожатого по обеспечению Интернет-безопасности»

Работу выполнили студенты ПС-ППБ-21:
Айсина Ольга, Богунова Алина,
Варакина Анастасия, Винокурова Виктория,
Ежова Екатерина, Сычева Наталия,
Тилицына Дарья, Филимонова Валерия

Интернет открыл новые возможности для коммуникации, теперь гораздо проще общаться и работать. Сегодня для реализации деятельности российского движения школьников, вожатства, волонтерства, благотворительности использование форм сетевого взаимодействия стало неотъемлемым условием. Однако надо понимать, что далеко не все образовательные организации готовы к построению сетевой системы внутренних и внешних коммуникаций.

Существует проблема в реализации такого взаимодействия вследствие низкого уровня владения педагогами информационными и коммуникационными технологиями, неумением использовать интернет для решения образовательных, культурных, социальных задач, а также проблема физического наличия интернета в информационной среде школы. При этом дети и молодежь используют интернет технологии куда как лучше взрослых, что делает их с одной стороны мобильными, а с другой – уязвимыми, т.к. информационное взаимодействие в сети скрывает довольно много опасностей.

Понимание того, как работают методы информационного воздействия, является основой для критического анализа действий в сети.

В соответствии с законодательством РФ под информационной безопасностью ребенка понимается состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью, физическому, психическому, духовному и нравственному развитию, в том числе информацией, распространяемой посредством сети Интернет.

В общем случае под риском или угрозой понимают возможность наступления некоего события, влекущего за собой негативные последствия.

Существует большое количество видов и методов манипулирования, которые широко описывает И.М. Ажмухамедов, мы рассмотрим некоторые из них и приведем примеры, адаптированные для школьников.

Психологическая атака – метод активного воздействия на психику человека, целью которого является отключение логического мышления. Человека побуждают к нужной реакции посредством произведения (отрицательного или положительного) или через введение в состояние растерянности. Например, школьник получает по электронной почте письмо, адрес которой можно легко узнать из открытых источников (социальные сети, блоги, форумы и проч.). В тексте злоумышленник с помощью психологического воздействия принуждает его к выполнению определенных действий (посылке, скачать или запустить программу, просто открыть прикрепленный файл и т.п.).

Пример легенды такой атаки:

Текст письма, где отправитель просит «жертву» помочь составить генеалогическое древо. Интересно, что их фамилии совпадают, и всего-то нужно посмотреть прикрепленный файл с общей родословной. На самом же деле к письму прикреплена ссылка для скачивания, активирующая вирус.

Атаки технического характера не столь страшны для физического здоровья, в отличие от атак психологических.

Например, **психологическое программирование** является методом однообразного или настойчивого воздействия на психику человека.

Цель такого воздействия – выработать алгоритм поведения и определенные образы мышления у «жертвы».

Примером психологического программирования может быть регулярная рассылка сообщений одной и той же тематики (например, с предложением участия в каких-нибудь квестах бесплатно). Допустим, что школьник, получив предложение интересного и бесплатного времяпрепровождения в первый раз, его проигнорировал.

Однако, получив несколько похожих сообщений с предложением бесплатной апробации нового квеста, промо-акции квеста в честь каникул или акции «приведи друзей и пройди сам квест бесплатно», он, возможно, задумается и все же выполнит указанные действия в инструкции.

За приведенными выше методами скрываются угрозы нового типа, к которым зачастую не готовы ни семья, ни школа, ни, конечно, сами дети. Это и суицидальные «игры», группы в социальных сетях, различные форумы, это сайты, распространяющие информацию о наркотиках, порнографии, разжигающие национальную рознь. Это экстремисты и террористы, которые занимаются вербовкой молодежи через социальные сети и мессенджеры, используя все те же манипулятивные технологии: вызвать доверие, чем-то заинтересовать, поддержать непонятого родителями, сверстниками, учителями подроста, чем-то помочь, что-то купить, просто встретиться погулять.

Цель виртуального «знакомого-друга» проникнуть в мысли собеседника, стать частью его существования и постепенно менять картину реальности, примеров тому множество. «Жертва» может долго не понимать, в какой «сети» она оказалась.

Для обеспечения информационной безопасности детей перед нами стоит общая задача правильно и оперативно оценить степень угрозы информации, которую они получают или передают.

Формирование основных навыков общения, отбора и обмена информацией возможно в различных формах: «в процессе учебной деятельности; во внеурочных формах работы; в форме личного общения «взрослый – ребенок»; через консультирование и информирование».

Алгоритм обеспечение медиабезопасности детей и молодежи в сети интернет:

ШАГ ПЕРВЫЙ.

Формирование осмысленного отношения к получаемой информации. Информационно-медийное сопровождение вожатской деятельности

ШАГ ВТОРОЙ.

Изучение нормативно-правовых документов по вопросам защиты детей от информации, причиняющих вред их здоровью и развитию.

ШАГ ТРЕТИЙ.

Обучение выявлению недостоверных или манипулятивных признаков информации на типичных примерах.

ШАГ ЧЕТВЕРТЫЙ.

Обучение основным технологиям противодействия недобросовестной информации.

ШАГ ПЯТЫЙ.

Обучение эффективному поиску дополнительной информации в сети интернет.

ШАГ ШЕСТОЙ.

Воспитание сетевого этикета.

Источник:

Информационно-медийное сопровождение вожатской деятельности: Методические рекомендации // Авторы-составители: Т. Н. Владимирова, А. В. Фефелкина / Под общей редакцией Т. Н. Владимировой. – Москва: МПГУ, 2017. – 54 с.

Спасибо за внимание!