«Цифровая культура поведения и онлайн угрозы»

Гусева О.А.

Традиционно сложилось, что вежливый человек – тот, кто не чавкает за столом, уступает место и приветливо здоровается при встрече. Однако для современного человека уже недостаточно соблюдать правила светского этикета, чтобы считаться культурным. Человеку, живущему в информационный век, теперь нужно еще соблюдать и цифровую культуру поведения.

Особенность цифровой культуры в том, что любое правило можно объяснить не только принципами вежливости и взаимного уважения, но и технологическими особенностями цифровой среды, цифровым пространством.

Цифровое пространство, создаваемое информационно-коммуникационными технологиями, способствует тому, что интернет прочно входит в повседневную жизнь большого количества людей и становится как системой, внутри которой осуществляется широкий спектр видов деятельности, так и средством для реализации этих видов деятельности.

По определению ректора ВШЭ понятие «Цифровая культура» — это умение работать с большими данными, умение вести поиск, умение отбирать нужную информацию в потоке данных… Это наиболее общие умения, которые должны формироваться в общеобразовательной школе. Вуз — поздновато для культуры выбора, культуры выхватывания нужной информации из огромного потока данных, которые нас окружают.”

Умение сортировать и искать информацию в большом потоке данных как в том же интернете, так и в литературных источниках это бесспорно важный скилл. Например, начиная со старших классов школы, ученикам уже необходимо уметь находить и подбирать наиболее оптимальный и подходящий материал для их восприятия при подготовке к экзаменам из огромного вороха всего.

Именно цифровая культура как система правил и норм онлайн-общения связанных с использованием цифровых технологий выступает важнейшим фактором профилактики и снижения онлайн угроз. В 2004 году даже появился «День безопасного Интернета» – международная дата, посвященная проблеме безопасности детей и взрослых в сети Интернет и формированию этичной и безопасной онлайн-среды. Отмечается в первый вторник февраля.

Ко Дню безопасного Интернета, компания Microsoft представила результаты ежегодного исследования, посвященного культуре общения и личной безопасности в сети за 2019 год. На его основе также был составлен рейтинг стран по индексу цифровой культуры (Digital Civility Index, DCI). Сегодня индекс составляет 70%, что является самым высоким показателем неуважительного обращения в сети с начала проведения исследования в 2016 году. За этот период количество онлайн-угроз увеличилось с 17 до 21.

**Какие есть Интернет-риски (угрозы)?**

Контентные риски – возникают в процессе использования материалов, содержащих противозаконную, неэтичную и вредоносную информацию (насилие, агрессию, угрозы сексуального характера, нецензурную лексику, пропаганду суицида, наркотических веществ).

Коммуникационные риски – связаны с межличностными отношениями Интернет-пользователей и включают в себя незаконные контакты (например, с целью встречи), кибербуллинг, грумминг.

Потребительские риски – злоупотребление правами потребителя (риск приобретения товаров низкого качества, подделок, контрафактной и фальсифицированной продукции, хищение денежных средств злоумышленником через онлайн-бакинг).

Технические риски – возможность повреждения программного обеспечения, информации, нарушение конфиденциальности, взлом аккаунта, хищение паролей и другой персональной информации.

Интернет-зависимость – непреодолимая тяга к чрезмерному использованию Интернета. В подростковой среде проявляется в форме увлечения видеоиграми, навязчивой потребности к общению в чатах, круглосуточном просмотре фильмов и сериалов в Сети.

По информации специальной линии «Дети – онлайн» по количеству обращений, связанных с различными Интернет – рисками на первом месте по числу обращений идут коммуникационные риски – 41 %, на втором – технические риски (32 %), на третьем – контентные риски (12 %), затем идут Интернет-зависимость (10%) и потребительские риски (5 %).

На какие риски нам, взрослым, необходимо обратить внимание для того, чтобы оградить наших детей?

Угроза первая — недетский контент. Этот тип угроз не нуждается в представлении. Все мы хотя бы раз натыкались в интернете на текст или картинки, которые потом хотелось «развидеть».
Чтобы оградить ребенка от нежелательного контента, нужно либо постоянно сидеть рядом с ним, либо использовать специальные программы родительского контроля.

Угроза вторая — анонимный недоброжелатель. Каждый ребенок, который общается в Интернете, зарегистрирован в соцсетях и использует мессенджеры, должен понимать, что не все виртуальные друзья — те, за кого себя выдают. Необходимо рассказать ребенку, что часто под видом его ровесников с ним могут общаться взрослые, преследующие самые разные цели. Поэтому важно уметь критически оценивать все, что пишут незнакомые люди (в личных сообщениях, в комментариях, на форумах и в чатах), и ни в коем случае не разглашать личную информацию о себе или о родителях.

Кибербуллинг, к сожалению, стал распространенным явлением. Суть его близка к обычной травле, нередко возникающей в коллективе несовершеннолетних. Жертвы кибербуллинга страдают от нападок в социальных сетях, угроз и оскорблений в личных сообщениях. Социальные сети сегодня стали для нас больше, чем просто среда общения и обмена фотографиями. Простота работы со своими страничками со смартфонов и планшетов, недорогие тарифы для подключения мобильного интернета и доступный wi-fi позволяют быть on-line всегда и везде, а социальные сети превращаются в устойчивую привычку, без которой мы уже не можем представить современную жизнь. Можно даже перефразировать известную поговорку: «Встречают по аватарке, а провожают по контенту».

Вот несколько простых правил безопасности интернет-пространстве, о которых должны знать мы и наши дети:

* Для защиты своего компьютера необходимо регулярное обновление программного обеспечения, использование надежных антивирусных и антишпионских программ.
* В Интернете не стоит переходить по ссылкам и нажимай кнопки во всплывающих сообщениях, которые кажутся подозрительными. Даже если вас будут уверять, что там находится нечто очень важное лично для вас.
* Для защиты личной информации придумайте надежный пароль и никому его не сообщайте. Для каждого ресурса стоит использовать уникальные логины и пароли.
* Никогда не предоставляйте секретные сведения, например, номер счета или пароль в ответе на сообщение электронной почты или в социальных сетях.
* Прежде чем вводить секретные сведения в веб-форме или на веб-странице, обратите внимание на наличие таких признаков, как адрес веб-страницы, начинающийся с префикса https и значка в виде закрытого замка рядом с адресной строкой, который обозначает безопасное соединение.
* Для безопасности общения в социальных сетях оставляйте как можно меньше данных о себе и избирательно подходите к предложениям о дружбе.
* Откройте пункт «Настройки» или «Параметры» в таких службах, как Facebook и Twitter, чтобы настроить список пользователей, которые могут просматривать ваш профиль или фотографии, помеченные вашим именем, контролировать способы поиска информации и добавления комментариев о вас, а также узнать, как можно заблокировать некоторых пользователей.
* Перед просмотром входящих писем на электронном ящике, проверьте адрес отправителя. Подозрительные письма смело отправляйте в спам, особенно если в таких письмах содержатся прикрепленные файлы.
* В чатах и системах мгновенного обмена сообщениями вы никогда не можете быть уверенными, кто с вами общается. Постарайтесь избегать общения с незнакомцами и ни в коем случае не соглашайтесь с ним на встречу в реальной жизни.
* Для скачивания картинки или мелодии вам предлагают отправить смс? Не спешите! Сначала проверьте этот номер в интернете — безопасен ли он и не обманут ли вас.