Безопасность детей в Интернете: что могут взрослые?

И. Н. Васильева, начальник управления информационных технологий и электронных образовательных ресурсов НИО

Тезис о том, что современные дети принадлежат к совершенно новому типу людей — digital Native — (Digital Native — термин, впервые использованный американцем Марком Пренски для обозначения людей, которые родились во время цифровой революции и находятся под воздействием цифровых технологий. Людей, которые родились до начала цифровой эпохи, Пренски назвал, соответственно, «цифровыми иммигрантами») – «цифровым аборигенам»*, становится совершенно очевидным. Стоит только удивляться скорости, с которой они осваивают современные гаджеты.

С гаджетами, кажется, всё понятно, но есть и другое «развлечение» — Интернет, который с каждым днём всё больше проникает во все сферы жизнедеятельности человека. Растёт и число пользователей сети. В связи с этим возникает вопрос: нужно ли разрешать детям пользоваться всемирной паутиной? Очень небольшая часть взрослой аудитории ответит отрицательно. Запретить пользоваться проще всего, однако, сколько времени продлится этот запрет? Большинство же без тени сомнения ответит утвердительно: Интернет позволяет детям обучаться, развиваться, учит виртуальному общению, которое стало неотъемлемой частью нашей жизни.

Взрослые привыкли заботиться о детях в повседневной жизни. А насколько комфортно им в цифровом мире? Надеемся, что материалы данной статьи помогут читателям разобраться, какие опасности для детей могут таиться во Всемирной паутине и что мы, взрослые, можем сделать для обеспечения их безопасности.

Детская аудитория: какая она?

Движение «Безопасность ребёнка в онлайновой среде» (Children-OnlineProitection — COP) разделило детскую аудиторию на группы: 5-7 лет, 8-12 лет и старше 13 лет, различающиеся по видам деятельности, которыми дети заняты в сети.

Дети 5-7 лет, как правило, проводят время за компьютером, играя. Это могут быть игры, которые инсталлируются на жёсткий диск компьютера и размещённые в сети. Что же такое сетевые игры?! Представьте себе ситуацию: вы отпускаете ребёнка погулять во двор, а через некоторое время он возвращается домой со слезами на глазах и без любимой игрушки. Что это значит? На детской площадке появились хулиганы! Первое желание родителя — выйти во двор, найти обидчика и восстановить справедливость. И в реальной жизни это вполне возможно, а в виртуальной — как?

Ещё один пример. Вдруг ваш ребёнок начинает фонтанировать невесть откуда почерпнутыми идеями: я могу выиграть денежный приз, мне надо срочно освоить приёмы тайского бокса и т. д., на воплощение которых срочно нужны деньги.

8-12-летние дети становятся не просто «игроками», они — активные пользователи социальных сетей, таких как «В контакте», «Одноклассники». Некоторые общаются в чатах, используют электронную почту. Отправить личное сообщение с оскорбительными или просто неприятными высказываниями — это мелкая шалость, но и она может здорово испортить настроение ребёнку.

Сегодня 13-летние ребята — это уверенные пользователи компьютера (в рамках удовлетворения своих познавательных запросов), азартные игроки, активные

«писатели» (более 60 % современных подростков ведут сетевые дневники «В контакте», Твиттер,
Фейсбук, ЖЖ и др.). Именно в этом возрасте дети активно загружают музыку, пользуются электронной почтой.
Вам приходилось оплачивать счета мобильных телефонов на шестизначные суммы?! Мы, взрослые, иногда сами попадаемся на эту удочку, а что говорить о детях!
Знают ли взрослые, что делают дети в Интернете?
Согласно социологическому исследованию, инициированному компанией «Киевстар» в 2009 г., 76 % родителей не знают, какие сайты посещают их дети. Но не это самое страшное, пугает другое – потенциальные жертвы реальных угроз сети: 17% детей готовы предоставить информацию о себе и своей семье – адрес, график работы родителей, наличие ценных вещей дома; 28% могут без колебаний послать свою фотографию незнакомцам; 22% попадают на сайты «для взрослых»; 14% время от времени присылают платные SMS для получения бонусов в онлайн-играх, не обращая внимания на стоимость этих сообщений. Так обстояли дела в 2009 году, а что сейчас?
В ходе реализации экспериментального проекта по апробации модели обучения с использованием индивидуальных электронных устройств в сентябре 2011 года (старт проекта) было проведено анкетирование родителей учащихся начальных классов. Большинство родителей согласны с тем, что Интернет оказывает на детей позитивное влияние, но многие задумываются и об угрозах Интернет-пространства. 64% родителей разрешают детям свободно пользоваться Интернетом, никак не ограничивают их во времени. Лишь 24% устанавливают временные ограничения и следят за тем, какие сайты посещают их дети; 28% стараются ввести правила пользования сетью. Большинство родителей (63%) сообщают, что не обладают достаточной информацией о том, как защитить своего ребёнка от негативного контента в Интернете. Почти треть (28%) не устанавливают правил работы ребёнка в сети.
Опасности и правила безопасности в Интернете
Всемирная сеть предлагает множество правил и рекомендаций по обеспечению безопасного использования глобальной сети детьми. Например:
* Общие правила безопасности в Интернете, сетевой этикет;
* Права детей в онлайне;
* Азартные игры и интернет-зависимость;
* Безопасное поведение в онлайн-играх;
* Безопасность в социальных сетях;
* Онлайн-пиратство (нелегальный контент), авторское право в интернете;
* Создание ощущения психологической связи, заботы, а также запугивание, противодействие им;
* Опасный (недетский) контент;
* Онлайн-коммерция, оплата услуг через SMS;
* Интернет-мошенничество, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям.
Какие меры следует предпринять?
Уменьшение опасностей при работе ребёнка в Интернете должно предусматривать: настройку контекстной фильтрации, ограничение времени пользования Интернетом,

контроль за посещаемыми ресурсами, просмотр его активности в социальных сетях и адресатов почтовых отправлений. И самое важное — откровенное общение с ребёнком:
обсуждение правил пользования Интернетом, возможных опасностей, которые его подстерегают, как правильно общаться, онлайн-опыт ребёнка (что его тревожит, было ему неприятно, непонятно и т. п.).
Какие решения предлагают компании-разработчики для обеспечения безопасности в Интернете?
Необходимо настроить:
* учётные записи пользователей (целесообразно создать для ребёнка отдельную учётную запись для входа на компьютер и произвести её настройки);
* браузер (например, в браузер Internet Explorer входит модуль «Ограничение доступа» (Content Advisor) — Сервис | Свойства обозревателя | Содержание (Tools | Internet Options | Content));
* программу родительского контроля (например, в операционной системе Windows Vista есть специальная утилита для родительского контроля, которая позволяет ограничить время работы за компьютером, сформировать «белые» и «чёрные» списки интернет-ресурсов);
* программы для защиты от вирусов и вредоносного программного обеспечения (например, Microsoft Security Essentials, Kaspersky Internet Security и др.);
* службы для обеспечения безопасности при работе в Интернете (Internet Security) (позволяют ограничить доступ с вашего компьютера к информации нежелательного характера);
* поисковую систему для работы в Интернете (можно использовать детский поисковик «Гогуль»);
* дополнительно установить специальную программу для контроля времени работы за компьютером (автоматически отключает доступ к сети при нарушении заданных ограничений: выход за рамки графика работы в сети, превышение лимита интернет-трафика и т. п.).
Что должны предпринять взрослые?
1. Не публикуйте полную личную информацию в Интернете, так как она может стать доступна преступникам или мошенникам.
2. Не посещайте подозрительные веб-сайты, не скачивайте с них файлы, не устанавливайте подозрительные программы.
3. Прежде чем загрузить на свой компьютер какой-либо файл, убедитесь, что ресурс надёжный, после скачивания — проверьте файл антивирусом.
4. Проводите проверку любого сменного носителя (дискета, лазерный диск, flash-память и др.).
5. Используйте антивирус на компьютере, регулярно обновляйте антивирусные базы.
6. Не отвечайте на письма с рекламными сообщениями (спам-письма).
7. Получив письмо от незнакомого отправителя, никогда не открывайте вложенные файлы — они могут быть заражены.
8. Не отвечайте на письма с просьбой перевести какую-либо сумму денег девушке (юноше) попавшему в беду (такие письма называются «нигерийские письма»).

9. Если на компьютере установлен антивирус: НЕ выключайте постоянную проверку; обновляйте антивирусные базы (не реже одного раза в три дня); проводите проверку всего диска каждую неделю.
10.Если ваш компьютер заражён (появляются рекламные сообщения, нельзя прочитать
документы) и у вас требуют деньги для «лечения» компьютера или расшифровки данных — ни в коем случае не отправляйте их.
11.Никогда не предоставляйте удалённый доступ к вашему компьютеру незнакомым людям.

Рекомендации для педагогов

При размещении информации об учащихся в сети Интернет:
* используйте минимум личной информации учеников для создания учётной записи в онлайн-инструментах. Выбирайте те инструменты, которые позволяют защитить личную информацию учеников;
* создавая онлайн информационные материалы для вики или блогов, внимательно относитесь к деталям. Никогда не выкладывайте в Интернете электронные адреса учеников, их пароли, номера телефонов или другую идентифицирующую информацию;
* в настоящее время считается, что публикация имён учеников в Интернете сопряжена с низким риском, при условии, что они не предоставляют никакой другой идентифицирующей информации. Подумайте, возможно, вам стоит разрешить вашим ученикам использовать их реальные имена и первые буквы фамилий в классных блогах и на групповых сайтах;
* правила использования ИКТ не позволяют выкладывать в Интернет фотографии учеников, демонстрирующие их лица. Если правила, принятые в вашей школе, позволяют делать это, не подписывайте имена учеников на фотографиях, вместо этого просто опишите, что они делают, показывают и т. д. Вы также можете вырезать фотографии таким образом, чтобы они были сфокусированы на деятельности учеников, а не на их лицах;
* при работе с блогами, вики, сайтами получите разрешение у родителей на регистрацию детей.

При проведении занятий с использованием Интернета:
* во время проведения занятий ведите контроль за использованием компьютера и сети Интернет учащимися;
* принимайте меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу;
* при обнаружении ресурса, который содержит информацию, запрещённую для распространения в соответствии с законодательством, или иного потенциально опасного для учащихся контента, сообщите об этом лицу, ответственному за работу Интернета и ограничение доступа.

Предостерегите учеников от предоставления персональной информации о себе или своих одноклассниках в анкетах, опросах или электронных письмах. Порекомендуйте им обращаться к учителю, родителям или другим надёжным взрослым в ситуациях, когда они не знают, как правильно поступить. Обсудите с детьми вопросы цифрового гражданства: выбор онлайн-имени, неразглашение персональной информации, права интеллектуальной собственности.

Рекомендации для родителей

* Настройте компьютер: программы родительского контроля, антивирусные программы, детские поисковые системы, настройки браузера.
* Наблюдайте за тем, что делает ребёнок в Интернете (расположите компьютер в месте общей доступности; обсуждайте с ребёнком, какие ресурсы он посещал, что его обеспокоило).
* Знакомьтесь с Интернетом вместе с ребёнком.
* Составьте вместе с ним правила пользования Интернетом или заключите джентльменское соглашение (какие сайты можно посещать, сколько времени можно работать, безопасный почтовый ящик).
* Обсудите с ребёнком правила безопасного поведения в Интернете (не встречаться с людьми, с которыми познакомился в сети; не размещать личной информации; сообщать взрослым, если что-то напугало или встревожило; не делать ничего, что требует оплаты; не переходить по рекламным ссылкам; не сообщать пароли).
* Научите ребёнка ответственному поведению в Интернете. Помните золотое правило: то, что вы не сказали бы человеку в лицо, не стоит отправлять ему по SMS, электронной почте или размещать в комментариях.
* Оценивайте интернет-контент критически. То, что содержится в Интернете, — не всегда правда. Дети должны научиться отличать надёжные источники информации от ненадёжных и проверять информацию, которую они находят в Интернете. Также объясните детям, что копирование и вставка содержания с чужих веб-сайтов могут быть признаны плагиатом.

Сайты, посвященные вопросам безопасной работы в Интернете http://mir.pravo.by/library/edu/roditel/ten — Детский правовой сайт (раздел «Десять правил безопасности для детей в Интернете»). http://www.onlandia.by/html/etusivu.htm — Онляндия — безопасная веб-страна (Онляндия — интерактивный курс по интернет-безопасности, предлагаемый офисом Microsoft для детей, родителей и педагогов по безопасности в Интернете). http://nonviolence.iatp.by/parents/safety.htm — сайт государственного общественного объединения «Дети не для насилия» (раздел «Безопасность ребёнка в Интернете»). http://www.microsoft.com/rus/childsafety — сайт «Безопасность детей в Интернете». http://www.microsoft.com/rus/athome/security — сайт «Безопасность дома». http://detionline.ru/ — сайт некоммерческой акции «Ребёнок в сети», проводимой PandaSoftware (перечень основных интернет-угроз, с которыми могут столкнуться дети, подсказки и советы для учителей, родителей и детей). http://www.securelist.com/ru/safeonline/rules — энциклопедия безопасности от Касперского. http://www.friendlyrunet.ru — фонд «Содействие развитию сети Интернет "Дружественный рунет"» http://detionline.eom/assets/files/journal/9/pract9.pdf — рекомендации в стихах для детей.

Что порекомендовать детям? http://www.onlandia.by/html/etusivu.htm (см. выше). http://gogul.tv/ — федеральная программа безопасного детского Интернета «Гогуль». http://www.smeshariki.rU/gamemain.aspx# — что нужно знать о безопасности, чтобы не попасть в плохую историю (советы от смешарика Пина). http://www.nesquik-club.com/ru/popup_play_safe_online.aspx — «Играй в сетевые игры безопасно» — советы для самых маленьких от NesquikClub. https://sites.google.com/site/detamobinternete/home — Интернет-букварь.

Как донести актуальный материал?

Привлечь внимание участников образовательного процесса к проблеме безопасного использования сети Интернет можно на педсоветах («Безопасный Интернет» как одна из
обсуждаемых тем); родительских собраниях; на отдельной страничке на сайте учреждения образования, блоге класса, творческой группы педагогов, родителей; путём проведения акций («Неделя безопасного использования Интернета»), подготовки стенных газет и информационных листков.

Обсудить предложенную тему, а также получить дополнительную информацию о безопасной работе в сети Интернет вы сможете на сайте http://www.avi.by/