Интернет-безопасность детей: что надо знать учителям

Диана Александровна Богданова,
старший научный сотрудник лаборатории проблем информатизации образования РАН, кандидат педагогических наук, dbogdanova@ipiran.ru

• *интернет-безопасность* • *интернет-риски* • *Whatsapp* • *Facebook* • *super-logoff* • *Chatroulette* • *Snapchat* • *Instagram* • *Four square* • *Flikr* • *родитель-«вертолёт»* •

Если в наши дни вдруг будет объявлено, что ДНК современного молодого человека состоит не из хромосом, а из айпи адресов, никто не удивится подобной шутке. Окружающая нас и наших детей действительность существенно изменилась. Интернет активно вошёл в жизнь даже старшего поколения, а дети давно живут «в расширенной реальности». Сейчас неправильно говорить «в реальной жизни», имея в виду офлайн. Facebook — это тоже реальная жизнь[1]. Изменился Интернет: он стал доступен везде, где есть мобильная связь.

К сожалению, наша школа изменилась мало. И на протяжении уже довольно долгого времени специалисты, работающие в области образования, ведут дискуссии о том, чему следует учить детей. Очевидно, что нынешняя школа по существующим программам и методикам отстаёт от веяний времени. По мнению специалистов в цифровую эпоху совершенно необходимы будут особые когнитивные умения, позволяющие успешно взаимодействовать с информацией в режиме реального времени. А люди, которые будут обладать умениями находить информацию, а также анализировать, структурировать и классифицировать её, бесспорно, будут иметь социальное, культурное и экономическое преимущество[2].

Одним из существенных когнитивных навыков специалисты считают оценку надёжности информации с учётом фактора времени, контекста и личной интерпретации. Это именно тот навык, который должен формироваться с начальной школы, и его значимость особенно возрастает с того момента, когда дети начинают свою жизнь в Интернете. Он напрямую связан, особенно в школьном возрасте, с медиаграмотностью и интернет-безопасностью. Кибербезопасность, е-безопасность, безопасный Интернет, безопасность он-лайн — вот перечень терминов, обозначающих в разных странах проблему, возникшую в последнее десятилетие в связи с работой детей в Интернете. Эта проблема сейчас актуальна как никогда. В ситуации, когда Интернет был привязан к компьютеру, находящемуся в определённом месте, решение проблемы безопасности представлялось более очевидным.

Два года назад специалисты советовали родителям держать компьютер, которым пользуется ребёнок, в общей комнате — для того, чтобы иметь возможность контролировать, какие сайты он посещает, с кем общается в сети. С появлением мобильных возможностей решение проблемы контроля усложнилось: стало очевидно, что меры только запретительного или ограничительного характера перестают быть эффективными. Считалось, что установки контентных фильтров в школах и на домашних компьютерах будет достаточно для регулирования доступа детей к ненадлежащей информации[3]. А сейчас ребёнок

[1] **Богданова Д.А.** Цифровой гражданин: ответственности школы и родителей //Дистанционное и виртуальное обучение, 2013. № 7. С. 95–109.

[2] **Богданова Д.А.** Образовательные парадигмы в цифровую эпоху // Problems of computer intellectualization. Sofia. C/o Jusautor 2012. С. 274–279.

[3] **Богданова Д.А.** О хранилищах образовательных ресурсов и е-безопасности (на примере Австралии и Великобритании) // Information models of knowledge. Киев: София, 2008. С.113–118.

может, используя свой мобильный телефон, выходить в сеть из любого места, не обязательно из дома или из школы. И если раньше активная роль по обеспечению безопасного пребывания ребёнка в Интернете отводилась только взрослым, то в новых условиях становится очевидной необходимость воспитания у детей навыков надлежащего ответственного использования технологий во всех аспектах повседневной жизни и деятельности.

В связи с этим тема «цифрового гражданства» становится всё более актуальной. Цифровое гражданство представляет собой концепцию, позволяющую учителям и специалистам в области информационных технологий понимать, *что* нужно знать учащимся, чтобы пользоваться технологиями надлежащим образом. Это способ подготовки учащихся к жизни в обществе, насыщенном технологиями. Цифровое гражданство сродни гражданству в реальной жизни: включает много обязанностей и даёт много преимуществ. Но особенным его делает тот факт, что оно гарантирует гораздо больше число соотечественников: порядка трёх миллиардов человек. Цифровое гражданство — это знание правил надлежащего ответственного использования технологий во всех аспектах повседневной жизни и деятельности. Это не просто знание онлайновых опасностей и умение их избегать. Это и участие в сетевых сообществах, и умение использовать интернет с позиций здравого смысла, творчески расширяя свой мир, не нанося при этом ущерба любого рода другим пользователям и вдохновляя их делать то же самое.

В России пока что нет государственной программы по формированию у детей навыков безопасного поведения в Интернете. В сентябре 2012 года вступил в действие Закон «О защите детей от информации, причиняющей вред их здоровью и развитию». В начале февраля нынешнего года вступил в действие Закон о досудебной блокировке сайтов с призывами к экстремизму и массовым беспорядкам. Но отсутствуют саморегулирующие соглашения между контент-провайдерами об основных принципах безопасной работы в социальной сетях, значительным образом способствующих обеспечению безопасности пользователей младшего возраста, зарегистрированных в сети. Подобные соглашения существуют, например, в Евросоюзе[4]. У нас пока что обучение детей правилам безопасного поведения — результат деятельности отдельных единичных структур, а также энтузиастов, разместивших на своих сайтах описание основных угроз и правил безопасности. Так, например, ведут работы в этом направлении Академия Касперского, компания «Майкрософт», Институт открытого образования.

Значительная роль в текущей ситуации принадлежит вовлечённости педагогов и родителей в использование Интернета детьми. Существующий так называемый «технологический разрыв» между поколениями усложняет участие родителей в занятиях детей. Дети — гораздо более продвинутые пользователи сетевых технологий, чем их родители, зачастую просто по той причине, что могут проводить в Интернете гораздо больше времени и гораздо активнее обмениваются информацией друг с другом. Необходимо вырабатывать у детей правила сознательного и ответственного поведения онлайн. Сложившаяся ситуация ставит на повестку дня необходимость обучения основам интернет-безопасности будущих учителей начальной и средней школы. А в настоящее время существует острая необходимость обучения работающих учителей в рамках повышения квалификации. Также необходимо обучение и руководства школы, и родителей.

Рассмотрим, что было бы полезно знать учителям на сегодняшний день по теме интернет-безопасности. Определённое внимание в публикациях уже было уделено описанию и классификации интернет-рисков как базовым знаниям в этом вопросе. Однако в связи с непрерывным развитием технологий происходят изменения в окружающем нас мире, предлагаются новые сервисы, возникают новые тенденции. Необходимо исследовать возникающие новинки с позиций возможных угроз для детей, а также быть в курсе мировых тенденций в этом вопросе. И этот факт не следует забывать при формировании обучающих программ для учителей, они должны постоянно дополняться и обновляться.

Классификация рисков будет представлена не очень под-

[4] **Богданова Д.А.** Слабое звено // Дистанционное и виртуальное обучение. 2012. № 3. С. 68–76.

робно, а основное внимание будет уделено анализу отдельных сервисов, сетей и иных инструментов общения, а также существующим в настоящее время тенденциям в этом вопросе.

Начнём с классификации интернет-рисков. Существующая классификация, известная как три «Си» (content, contact, conduct), была разработана специалистами из Лондонской школы экономики[5]. Она представляет собой двухмерную модель, учитывающую участие (или роль) ребёнка и содержание самого риска. Структура достаточно полно охватывает существующие разновидности рисков и составляет хороший тандем вместе с традиционной классификацией по содержательной компоненте[6].

В соответствии с приведённой классификацией роль или позиция ребёнка в рисках меняется. Очевидно, что ребёнок школьного возраста в большинстве случаев становится жертвой или собственного заблуждения, или обмана. Таким образом, возникающие ситуации угроз, в которые вовлекается ребёнок, попадают преимущественно под контентные (1.2–1.4) и контактные (2.2–2.4) риски. В ситуации поведенческих рисков в силу собственной активной роли ребёнок из жертвы переходит в разряд активных действующих лиц и применительно к этой группе чаще всего проявляет себя в отдельных действиях, связанных с нарушением закона (3.2), и в других действиях (3.3–3.4). Для применения в практической работе классификация рисков по их содержанию даёт более крупные блоки, более удобна, и именно в соответствии с классификацией риски будут рассмотрены далее.

Ненадлежащее содержание *(1.2–1.4)*

Далеко не все материалы, размещаемые в Интернете, должны быть доступны для детей и молодёжи. Существуют сайты, пропагандирующие самоубийство, анорексию, сектантство. В силу возраста и недостатка жизненного опыта дети не в состоянии реалистично оценить все риски, связанные с содержимым материалов, размещённых на подобных сайтах. Нередко сайт, созданный первоначально с невинными целями, привлекает внимание пользователей с отклонениями психики — педофилов, эксгибиционистов — и начинает использоваться в целях, отличных от первоначальных[7].

Травля, запугивание (bullying) *(2.3, 3.3)*

Травля в детских коллективах существовала и раньше, но сейчас она приобрела изощрённые формы. Существует и скорбный список жертв кибертравли — детей, покончив-

Таблица 1

Классификация рисков, предложенная Лондонской школой экономики

№ п/п	Риски	Коммерческие	Агрессивные	Сексуальные	Оказываемое воздействие
1	Контентные (ребёнок является пассивным получателем)	Реклама, спам	Информация, связанная с насилием или проявлениями ненависти	Порнография или иной нежелательный контент	Предубеждение, расизм, вводящая в заблуждение информация
2	Контактные или коммуникационные (ребёнок выступает как участник)	Харвестинг (сбор личных данных), преследование, персональные данные, спонсорство	Подвергается буллингу или преследованиям	Встречается с незнакомцами, становится объектом ухаживания	Причинение вреда себе, сектантство, анорексия. Нежелательные убеждения, интернет-зависимость
3	Поведенческие (ребёнок проявляет себя как активное действующее лицо)	Нелегальное скачивание, азартные игры, терроризм, финансовые махинации	Буллинг или домогательсва по отношению к другому	Создание и размещение неподобающего материала	Предоставление неверной информации

[5] **Livingstone S., Haddon L., Gorzig A., Olaffson K.** Risks and safety on the Internet. The perspective of European children. Full findings. LSE, London, EU Kids Online. http://eprints.lse.ac.uk/27052/1/Comparing_Online_Risks_(LSERO). 2011.

[6] **Богданова Д.А., Федосеев А.А.** Внимание- Интернет // Открытое образование. 2010. № 2. С. 89–99.

[7] Там же.

ших жизнь самоубийством в результате буллинга. На фоне бурного развития секстинга (обмена посланиями сексуального характера) возник новый термин — slut shaming, который на русский язык перевести непросто. Порочащая девушку фотография или видео сексуального характера размещается в сети или рассылается среди общих знакомых. По своей сути это новый вид травли, использующий секстинг. Три фактора являются причиной столь широко распространённого в последнее время сексуального поведения подростков. Первый — это гиперсексуализация средств массовой информации, включая рекламу, второй — лёгкий доступ к порнографии, что особенно привлекает мальчиков 10–13 лет, и третий — мобильные телефоны, позволяющие очень просто делать фотографии с возможностью размещения в Интернете. Дети становятся порнографами, не имея понятия о любви и уважении в сексе.

В Великобритании начали борьбу с этой эпидемией. В конце марта текущего года британским школам был разослан документ, инициированный и разработанный Национальным обществом защиты детей от грубого обращения (NSPCC), Национальной ассоциацией директоров школ (NAH) и целым рядом других организаций. Документ даёт право учителю конфисковать, просматривать содержимое телефона ученика, заподозренного в распространении посланий сексуального характера. В случае обнаружения ненадлежащих материалов учитель обязан сообщить в полицию, руководству школы и родителям ученика.

Безопасность личной информации *(2.2–2.4)*

И педагоги, и дети, и родители должны знать о том, насколько бывает опасным размещение в Интернете персональных данных. Это может быть не только имя и фамилия, но и другая информация, о чём будет сказано дальше. Автор проанализировал значительное количество сайтов российских школ с позиций соответствия российскому Закону «Об образовании» и «О персональных данных». Обнаружилось, что школы на своих сайтах, помимо рекламы, не задумываясь, размещают в открытом доступе фотографии и списки классов, списки родителей. Очевидно, что разработка школьного сайта — один из первых шагов развития информационной среды образовательного учреждения. Однако созданная среда не должна содержать угрозы для безопасности ребёнка[8].

Заигрывание (grooming) *(2.4)*

Общаясь, дети заводят новые знакомства, принимая на веру, без критики, всю информацию, которую сообщает о себе новый «друг». Среда общения в этих сетях совершенно разнородная, а под прозвищами и аватарами могут скрываться люди не обязательно одного возраста или общего круга интересов. Дети должны знать, что никогда не следует идти на встречу с новым интернет-«другом» одному, не проинформировав об этом никого из взрослых. А опросы показывают, что подростки не считают новых онлайновых друзей потенциально опасными, и 12% встречались оффлайн с теми, с кем они познакомились онлайн. 21,5% подростков размещают в сетях собственные фотографии, не считая, что это опасно. И число таких поступков растёт экспоненциально с развитием социальных сетей. А 73,5% родителей полагают, что их дети знают, как грамотно вести себя в сети, и следуют этому[9].

Нарушение авторских прав *(3.2)*

Нелегальное скачивание фильмов, музыки, текстов, фотографий — повсеместная, не только российская проблема. При этом нередко используются технологии P2P (peer-to-peer), когда компьютеры связываются напрямую, что к тому же повышает и возможность заражения компьютера, создаёт предпосылки для использования программ-шпионов[10].

Интернет-зависимость *(2.5)*

Часто негативно отражается на успехах в учёбе, а иногда и на социальном поведении учащихся.

Безопасность компьютеров

В школе должны существовать правила работы за компьютером, обязательные как для сотрудников, так и для учащихся. А дома родителям необходимо научить детей правилам безопасного серфинга в Интернете и применению их для личных устройств — компьютеров, телефонов.

[8] **Богданова Д.А.** Какой он, сегодняшний школьный сайт? // Дистанционное и виртуальное обучение. 2012. № 5. С. 50–60.

[9] Social Networks: A Parent's Responsibility. http://sociallyactive.com/social-networks-a-parents-responsibility/

[10] **Богданова Д.А., Лисицына А.А.** В Интернет — с широко закрытыми глазами // Дистанционное и виртуальное обучение 2011. № 2. С. 117–125.

В последние годы специалисты заговорили о том, что обучение детей программированию с раннего возраста поможет проще научить их пониманию структуры Интернета, что будет способствовать повышению уровня медиаграмотности и знаний детей в вопросах интернет-безопасности. Одним из пионеров этого движения стала Эстония. К началу 2013–2014 учебного года для работы с детьми по этому новому направлению прошли обучение около 60 учителей начальной школы. Сначала в соответствии с решением Министерства образования и науки Эстонии дети будут осваивать основы программирования в среде, которая называется Tiger Leap, разработанной одноимённым фондом, как часть обычной школьной программы. После этого они могут продолжить занятия в клубах программирования. Tiger Leap пока что не имеет договорённостей о расширении пилотного проекта до уровня обязательной государственной учебной программы, однако очевидно, что это — первый серьёзный шаг в направлении медиаграмотности и интернет-безопасности[11]. Великобритания объявила в конце прошлого года о новом экзамене CGSE для выпускников школ по программированию.

Если же специалисты не пришли к решению о необходимости всеобщего обучения программированию, то что надлежит знать учителям, чтобы учить детей?

Учителям следует знать правила грамотного пользовательского поведения в сетях и сервисах и рассказывать о них детям. Нельзя не сказать о наметившейся в последнее время тенденции перехода подростков с Facebook на мобильные приложения[12]. В ноябре 2013 года Facebook объявил о снижении количества ежедневных посетителей, особенно из числа молодёжи. Фактически молодые люди всё ещё являются пользователями сети, но значительно снизили интенсивность пользования. Произошедшее — знаковое заявление, поскольку эта демографическая группа отражает наступающие изменения. Известно, что Facebook потерял значительное количество своих подписчиков после разоблачений Сноудена. А в последнее время подростки и молодёжь переключаются на использование мобильных приложений, таких как WhatsApp или на национальные аналоги, популярные в их стране, что, с точки зрения специалистов, снижает детские риски, связанные с социальными сетями.

Теперь, продолжая использовать Facebook как средство общения, молодёжь постепенно переносит основное направление своего интереса на мобильные телефоны. WhatsApp — самое популярное мобильное приложение в Великобритании и, по данным Mobile Marketing Magazine[13], имеет порядка 350 миллионов активных пользователей по всему миру. Это делает его самым популярным среди пользователей приложением для обмена сообщениями. Оно даже более популярно, чем Twitter, который насчитывает порядка 218 миллионов. По данным компании Tyntec[14] порядка 90% населения Бразилии, три четверти российских пользователей, половина британцев используют смс-приложения. WhatsApp установлено на более чем 85% всех смартфонов в Испании. И подавляющее большинство пользователей этих приложений составляют люди моложе 25 лет.

Новые сервисы, подобные WhatsApp, обладают неоспоримыми преимуществами конфиденциальности и отсутствием навязываемой рекламы. Аналитическая служба mobileYouth[15] считает, что по этой же причине около 80% подростков и молодых людей используют мобильные смс-сервисы, чтобы договориться о встрече. Другим существенным фактором, оказывающим влияние, является растущая популярность «селфи» и «луков»: фотографий себя самого, нередко смешных, снятых на мобильный телефон с расстояния вытянутой руки или фотографий в полный рост. По данным mobile Youth, практически половину фотографий, поступающих в Instagram от британских пользователей возраста от 14–21 года, составляют селфи. Отправка таких фотографий через мобильные сервисы гораздо безопаснее «вещания» на Facebook, особенно с учётом того фактора, что их не увидит ни началь-

[11] **Березина Н.Л., Богданова Д.А.** Об опыте обучения детей Интернет-безопасности // Информатика в школе: прошлое, настоящее, будущее всероссийская научно-практическая конференция, Пермь, 2014 (в печати).

[12] **Богданова Д.А.** Молодежь переходит на мобильные приложения //Новые информационные технологии в образовании, Екатеринбург 2014 (в печати).

[13] mobilemarketingmagazine.com

[14] http://www.tyntec.com/press/press-releases.html

[15] http://www.mobileyouth.org/stats-and-facts

ник, ни десятки «друзей», о которых и думать забыл. Селфи ещё более популярны на Snapchat, сервисе, через несколько секунд удаляющем фотографию после того, как она была просмотрена. Об этом сервисе подробнее будет сказано далее.

Помимо конфиденциальности, ещё одной из причин, по которым молодёжь начинает больше тяготеть к мобильным приложениям, является тот факт, что это не просто обмен сообщениями. Перечень предлагаемых услуг включает, помимо смс-сервисов, игры, стикеры и возможность обмена музыкой. Это пока что видимая тенденция, но никто не берётся предсказать дальнейшую судьбу этих сервисов. На настоящий момент известно только, что WhatsApp отвергла предложение Facebook купить компанию за 3 миллиарда долларов.

Рассмотрим теперь некоторые приёмы и правила работы в социальных сетях и мобильных сервисах, которые могут помочь минимизировать перечисленные выше риски и быть полезными как детям, так и учителям. Именно с этих позиций рассмотрим Facebook, Flickr, Instagram и другие.

Facebook

Собираясь выйти из сети, можно дезактивировать свой аккаунт. Дезактивация аккаунта не удаляет его. Подключившись обратно, пользователь сможет его реактивировать и восстановить все связи со своими друзьями. Когда же он не в сети, никто не может оставить записи на стене, или отправить частное сообщение, или просматривать содержимое. Во время пребывания пользователя в сети, посетители могут это сделать, но он сможет сразу же удалить всё то, что ему не понравится. Подобная практика называется super log-off. Пользователь не пытается таким образом избавиться от своих данных или обидеть своих друзей. Он просто минимизирует риск во время своего отсутствия. Гораздо проще дезактивировать аккаунт, чем каждый день менять личные настройки. Найти пользователя невозможно, если он в этот момент не в сети. Он невидим, если только не подключился. А когда он в сети, его друзья знают об этом. Это — стратегия минимизации возможных рисков и защиты в случае посещения аккаунта нежелательными посетителями. Таким образом, пользователь использует преимущества, которые даёт Facebook, и минимизирует риски во время своего отсутствия.

Другой способ существования — удаление всех посланий, всех записей и «лайков» вскоре после их появления. Таким образом, записи обновляются по мере их появления, старые удаляются. После прочтения всех комментариев они также удаляются. На несколько дней оставляются лайки, а затем и они удаляются. Люди очень любопытны, и, если хранить архивы, можно попасть в неприятную ситуацию только из-за того, что было написано давно, и о чём уже забыто. Если это важно, то оно сохраняется, всё устаревшее удаляется. И такая тактика не ставит задачей уберечь себя от внимания взрослых. Она помогает свести на «нет» риск быть неправильно понятым друзьями, что впоследствии неизбежно приведёт к выяснению отношений. Причём пользователь, о котором идёт речь, отправляет около 120 посланий в день. И он строго дифференцирует близких друзей и школьное окружение. С близкими друзьями можно обмениваться смс-ками по мобильному телефону, а пребывание в Facebook позволяет оставаться в курсе школьной жизни, поддерживать отношения с теми, кто уже окончил школу или с тем, с кем недостаточно хорошо знаком. Очевидно, что оба варианта существования имеют глубокий смысл и не требуют постоянного пребывания начеку из-за неосторожного поведения в сети: там меры предосторожности уже были приняты[16].

Flikr *(2.2–2.4)*

Социальный сервис Flickr предназначен для хранения и дальнейшего использования фотографий и видеороликов. К каждой фотографии её хозяин может добавить различные метки, включая фамилии людей, изображённых на ней. Пользователи системы могут образовывать группы по интересам, приглашать в группу других пользователей. А если в качестве меток используются фамилии, то можно легко найти фото человека, даже если вместо его фотографии в социальной сети используется аватар. Поэтому в качестве меток следует указывать не полные имена, а, возможно, просто имена или прозвища. В случае, если для места, где сделаны фотографии, определены точные GPS

[16] **Богданова Д.А.** Цифровой гражданин: ответственности школы и родителей // Дистанционное и виртуальное обучение. 2013. № 7. С. 95–109.

координаты, то они иногда тоже добавляются в качестве меток. Но в связи с широким распространением селфи, луков и навигационных сервисов, указывающих координаты, рекомендуется на время съёмок не включать навигационную опцию[17].

Google locator, I can stalk you, Foursquare (2.2)

Целый ряд идентичных сервисов и сайтов — Google locator, I can stalk you, Foursquare, используя возможности технологии Geolocation, определяют и фиксируют по GPS координатам или по метаданным отснятой фотографии либо место, где была сделана фотография, либо местонахождение мобильного телефона, владельцем которого является ребёнок, и размещают эти данные у себя. И опасность состоит в том, что можно узнать места, которые ребёнок часто посещает. Более того, отмечая своё присутствие, ребёнок нередко указывает и координаты своего дома — таким образом, становится известен его адрес. Чтобы сделать информацию недоступной для незнакомых людей, пользователю необходимо изменить свои настройки.

Однако дети, как правило, не задумываются об этом, и следует обратить их внимание на возможную опасность. Проблема может быть и в том, что они зачастую не знают, каким образом изменить настройки. Дети нередко воспринимают своё общение в Интернете как увлекательную игру, не сознавая, насколько виртуальный мир связан с реальным. Рассмотрим возможный сценарий поведения заинтересованного лица, пользователя Foursquare. Он пришёл в некое место, зарегистрировался и обнаружил, что в этом заведении уже находятся и другие пользователи. Посмотрев список, он, к примеру, обратил внимание на фотографию девушки. Просмотрев информацию о ней, он увидел список мест, где она отмечается чаще других пользователей, и получила (mayership) — «мэрство». В большинстве случаев, в зависимости от возраста, это будет дом, школа, вуз. Базовая информация собрана, а дальнейшие действия — на усмотрение пользователя.

Instagram

Социальная сеть Instagram появилась в 2010 году первоначально как платформа для обмена фотографиями среди пользователей сети, но с тех пор разрослась за счёт подключения различных социальных медиа, включая Twitter и Facebook. В 2012 году она была куплена Facebook, и начала стремительно набирать популярность. Компанией были объявлены новые правила обслуживания, позволявшие перепродажу прав на размещённые фотографии. Но незамедлительная протестная реакция общественности заставила новых владельцев отказаться от публикации фотографий. Приложения позволяют редактировать фотографии, снятые телефоном, и размещать их в сети.

Всё выглядит вполне невинным. Но, как всегда дьявол кроется в деталях. Как и в случае большинства социальных сетей, при регистрации требуется учётное имя. В этом случае дети должны знать, что необязательно давать свои имя и фамилию, а следует заменять их псевдонимом, и уж ни в коем случае не следует заполнять необязательные поля. Существуют возможности настроек конфиденциальности, ограничивающих доступ посторонних к просмотру фотографий, и по аналогии с Facebook, незнакомец должен первоначально отправить запрос на получение доступа. Но известно, что любители сайтов свиданий и фотографий «в бикини» регистрируются под вымышленными именами, выдавая себя за того, кем на самом деле не являются. Также известно, что настройки конфиденциальности не являются полноценной защитой. Существует возможность стать «последователем» (follower), что даёт доступ к содержимому даже после введённых настроек. Кроме того, если аккаунт соединён с Facebook или Twitter, необходимо проконтролировать настройки конфиденциальности и там. Кроме этого, надо твёрдо быть уверенным в том, что настройки у друзей также выставлены надлежащим образом[18].

Snapchat

Увлечение последнего времени, упоминавшееся выше, захватившее молодёжь: это управляемая передача фотосообщений — приложение для смартфонов. Владелец смартфона может снять фото или видео, снабдить его текстом и отправить адресату, указав при этом время, через которое это послание исчезнет из телефона получателя. Спустя заданное время фото действительно как бы исчезает навсегда. Этот сервис произвёл буквально революцию среди 13–25-летних, пересылая, по данным служ-

[17] **Богданова Д.А.** О подготовке и повышении квалификации педагогических кадров по вопросам интернет-безопасности // Образования — 2012. Педагогические основы разработки и использования электронных образовательных ресурсов. Матер. Междунар. науч. конф. (Минск. 24–27 октября 2012 г.). С. 36–40.

[18] Там же.

бы Snapchat, около 50 миллионов снимков ежедневно и позволяя, таким образом, «безопасно» обмениваться временами смешными, а временами — непристойными посланиями. Дети фотографируются в классе, сидя в одиночестве или с друзьями.

Основная цель этого сервиса — веселье, шутки. Но дети начали использовать его и для неприличных посланий, не задумываясь о возможных рисках. С помощью несложного поиска на Google можно легко узнать, как сохранить фото или видео без ведома отправителя. Можно сделать фотографию с экрана. Известно, что фотографии в Интернете не исчезают, а, попав туда, остаются навсегда. Если подобные фото сохранены, а затем обнародованы, это может нанести удар по семье, а репутация ребёнка может быть навсегда испорчена.

Chatroulette

Сайт был разработан московским школьником Андреем Терновским. Его название возникло после просмотра фильма о вьетнамской войне, где герои фильма — заключённые — играли в русскую рулетку. Главное его направление — общение между людьми всей планеты на основе вэбкамеры, микрофона или просто печати с помощью клавиатуры. Люди соединяются случайным образом, выбор происходит среди подписчиков сайта. Первоначальная идея и быстрый рост популярности — от 500 визитов в день в течение первого месяца до 50 000 через месяц — привели к тому, что теперь 35 000 человек могут связываться напрямую в каждый момент времени. Однако созданный с добрыми намерениями сайт начал использоваться отдельными посетителями с неблаговидными целями.

Примерно один из восьми участников соединения предстаёт обнажённым, демонстрируя себя либо своё участие в сексуальном акте. Университет Колорадо даже разработал программу, позволяющую различать лицо, глаза, кожу. А далее программа определяет, не ведёт ли себя пользователь перед камерой ненадлежащим образом, и позволяет блокировать изображение. Любопытно, что для решения этой проблемы потребовались специальные технологии, не известные ранее: анализ движущегося изображения, полученного с вэбкамеры. Ранее существовавшие программы работали со статичными изображениями высокого разрешения[19]. Но технологии развиваются, возникают новые сервисы, молодёжь их осваивает раньше других. И хорошо бы в структуре образования иметь службы, которые исследовали бы новые сервисы с позиций возможных угроз, и информировали бы заинтересованную образовательную общественность.

Как поступать с родителями и родителям

Исследования показывают, что родители представляют собой довольно инертную, сложную для работы группу, обременённую синдромом «не мой ребёнок» и не желающую прилюдно признать собственную недостаточную компетентность в проблеме «ребёнок и Интернет»[20]. Школам необходимо постоянно проводить разъяснительную работу с родителями, привлекая их к участию в решении возникающих проблем. Как уже было сказано ранее, препятствием в этом вопросе зачастую является «технологический разрыв» поколений — дети знают и умеют гораздо больше, чем их родители. В этом случае можно посоветовать родителям обратиться к ребёнку с просьбой научить пользованию тем или иным сервисом.

В последнее время многие родители в Великобритании, США регистрируются в тех же социальных сетях, которые посещает их ребёнок. Это позволяет отслеживать, как ребёнок ведёт себя в сети, с кем общается. Но эффект от этого можно получить только в случае доверительных отношений с ребёнком и собственного разумного поведения. Получивший новое звучание термин — «helicopter parent» — «родитель-вертолёт» — обозначает родителя, который сверхактивно контролирует жизнь своего ребёнка. Поэтому дети находят способы противостоять подобному родительскому контролю: исключают родителя из списка друзей или регистрируются в сети под вымышленным именем, которое становится известно только его друзьям. А теперь ещё и переключаются на мессенджевые сервисы типа Whatsapp, о чём говорилось ранее.

Основной тезис, который требуется донести до родителей: необходимость построения доверительных уважительных отношений с ребёнком. Только во время спокойных бесед и разбора примеров можно привлечь внимание ребёнка к проблеме. ❑

[19] **Moore R.J.** Chatroulette Is 89 Percent Male, 47 Percent American, And 13 Percent Perverts». TechCrunch 2010, March, 16.

[20] **Богданова Д.А.** Слабое звено // Дистанционное и виртуальное обучение. 2012. № 3. С. 68–76.