

ОТ ИНТЕРНЕТ-РИСКОВ – к цифровому гражданству



Диана Александровна Богданова,
старший научный сотрудник Института кибернетики
и образовательной информатики Федерального
исследовательского центра «Информатика
и управление» Российской академии наук,
кандидат педагогических наук



Галина Ростиславовна Буркатовская,
заместитель директора Центра образовательных
инфотехнологий Архангельского областного
института открытого образования

Окружающая нас и наших детей действительность существенно изменилась. Интернет активно вошёл в жизнь даже старшего поколения, а дети давно живут «в расширенной реальности» (augmented reality). Сейчас неверно говорить «в реальной жизни», оффлайн. Facebook — это тоже реальная жизнь. Изменился Интернет: он стал доступен везде, где есть мобильная связь¹. С его приходом исчезли множественные пространственно-временные барьеры, и мы в общении

¹ Богданова Д.А. Интернет-безопасность детей: что надо знать взрослым // Школьные технологии. — 2014. — № 2. — С. 98–105.

перестали быть привязанными только к тем, кто физически находится в непосредственном окружении: у нас появилась возможность устанавливать мобильные связи по всему миру, возможность учиться дистанционно. Интернет обеспечил учителей доступом к огромному количеству информации и образовательного материала, а учащихся — практически неограниченными возможностями для поиска информации в Сети.

• интернет-безопасность • интернет-риски • классификация интернет-рисков три «си» • цифровое гражданство • персональные данные • цифровые следы • секстинг • кибербуллинг • цифровая репутация • благополучие онлайн • цифровое благополучие

Жизнь в цифровую эпоху

По мнению сэра Кена Робинсона, «наши дети живут в самый интенсивный стимулирующий период времени за всю историю развития человечества. Образование более не ограничено стенами классной комнаты»². И на протяжении уже довольно долгого времени специалисты, работающие в области образования, ведут дискуссии о том, чему и как следует учить детей. 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 преимущество³. Поэтому необходимо стремиться к тому, чтобы учащиеся научились разумно «просеивать» изобилие найденной информации, и управлять навигацией в интернет-пространстве таким образом, чтобы это способствовало их обучению⁴. Однако вместе с технологиями пришёл и довольно внуши-

тельный список рисков, связанных с их использованием. Специалистами Лондонской школы экономики риски идентифицированы, исследованы и классифицированы⁵. Эта классификация, известная как три «Си» (content, contact, conduct), представляет собой двухмерную модель, учитывающую участие (или роль) ребёнка и содержание самого риска. Структура достаточно полно охватывает существующие разновидности рисков.

В табл. 1 приведена классификация рисков, предложенная Лондонской школой экономики.

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 которых оказывается 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 все-

² Ken Robinson Changing education paradigm TED video posted October 2010. Режим доступа: http://www.ted.com/talks/ken_robinson_changing_education_paradigm (Последнее посещение 10.10.2017)

³ Богданова Д.А. Образовательные парадигмы в цифровую эпоху // Problems of computer intellectualization. Sofia, C/o Jusautor 2012, — С. 274–279.

⁴ Johnson L., Adams S., and Haywood K. The NMC Horizon Report: 2011 K-12 Edition, (New Media Consortium: 2011). Режим доступа: <http://media.nmc.org/iTunesU/HR-K12/2011/2011-Horizon-Report-K12.pdf>. (Последнее посещение 10.10.2017).

⁵ Livingstone S., Haddon L., Gorzig A., and Olafsson K., (2011) Risks and safety on the Internet. The perspective of European children. Full findings. LSE, London, EU Kids Online. Режим доступа: [http://eprints.lse.ac.uk/27052/1/Comparing_Online_Risks_\(LSERO\)](http://eprints.lse.ac.uk/27052/1/Comparing_Online_Risks_(LSERO)) (Последнее посещение 10.10.2017).

Таблица 1

	1	2	3	4	5
		Коммерческие	Агрессивные	Сексуальные	Оказываемое воздействие
1	Контентные (ребёнок — пассивный получатель)	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, сектанство, анорексия. Нежелательные убеждения, интернет-зависимость
3	Поведенческие (ребёнок — активное действующее лицо)	Нелегальное скачивание, азартные игры, терроризм, финансовые махинации	Буллинг или домогательства по отношению к другому	Создание и размещение неподобающего материала	Предоставление неверной информации

го проявляет себя в отдельных действиях, связанных с нарушением закона (3.2), и в других действиях (3.3–3.4).

Время настоятельно требует, что школы должны начать учить детей, как учиться в сетевую эпоху, действуя в онлайн-пространстве позитивно, ответственно и безопасно.

Современные дети практически с раннего возраста начинают пользоваться Интернетом. Как правило, учащиеся старших классов начальной школы уже владеют набором пользовательских навыков. Однако умение использовать технологии для личных целей не означает, что они могут без затруднения начать использовать их для обучения, для исследований, делая это грамотно, эффективно и ответственно: они не получают таких знаний, пользуясь Интернетом дома. Например, они не задумываются о необходимости верификации найденной информации. Очень немногие дети понимают коммерческие аспекты Интернета. Они наивно полагают, что социальные сети созданы для того, чтобы дать им возможность общаться. Они не задумываются, что, анализируя соотношение позитивных и негативных постов в социальных сетях, бизнес-компании оценивают, насколько жители конкретной территории расположены к совершению крупных покупок. Они играют

в игры, где виртуальные возможности покупаются за реальные деньги. Не задумываются и о том, что компании собирают и делятся коммерческой информацией, получаемой на основании анализа пользовательских действий в сетях. Периодически мы узнаём о том, что молодые люди используют цифровой инструментарий ненадлежащим образом: для секстинга, кибербуллинга, обмана, для видеозаписи драк со сверстниками или плагиата. К сожалению, подобное поведение становится довольно распространённым, так как детей не приучают думать о том, какие цифровые следы они оставляют в Интернете и как это сказывается на их сетевой репутации. Учащиеся должны сознавать, что все материалы, размещаемые в Интернете, обладают четырьмя важными качествами: сохранность — они автоматически записываются и архивируются; воссоздаваемость — содержимое, созданное из битов, может быть дублировано; масштабируемость — потенциальная возможность распространения контента в сетевых сообществах велика; доступность — доступ к сетевым публикациям можно получить через поиск. Эти особенности онлайн-пространства означают, что детей

необходимо научить анализировать, какой вклад, положительный или отрицательный, внесёт в их цифровые следы, в их цифровую репутацию каждый материал, который они размещают.

Сейчас учащиеся с мобильных телефонов могут получить доступ в онлайн-пространство во время уроков, обходя школьные фильтры. И это делает невозможным решение проблемы безопасного Интернета за счёт ограничения Wi-Fi или фильтрации. В этом смысле в западных школах начал практиковаться подход BYOD (bring your own device — приноси своё собственное устройство), позволяющий использовать в классе те же устройства, которыми дети пользуются дома. Нам, взрослым, необходимо подумать, как правильнее воспринимать жизнь наших учащихся в Интернете: как две отдельные — школьную и домашнюю, или как одну. Подход «двух жизней» предполагает, что изучение вопросов, связанных с социальными, личными и экологическими последствиями технологического образа жизни, не имеет места в школе, оставляя детям возможность справляться самим, когда они сталкиваются с проблемами цифрового мира. В то же время подход «одной жизни» говорит о практических и педагогических преимуществах: учителя не только формируют у детей навыки ответственного поведения в Сети, они ещё способствуют строительству «мостика» между домом и школой. Поэтому включение в школьную программу основ цифрового гражданства будет способствовать и преодолению дистанции между школой и домом.

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 осо-

бенно возрастает с того момента, как дети начинают жизнь в Интернете. И он напрямую связан, особенно в школьном возрасте, с медиаграмотностью и интернет-безопасностью. Такой запрос требует реализации комплексного подхода к обучению позитивному, ответственному и безопасному поведению в Интернете. В связи с этим концепция «цифрового гражданства» становится всё более актуальной⁷.

Цифровое гражданство

Чтобы понять концепцию цифрового гражданства, полезно начать с первоначальной идеи. Гражданство в его традиционном смысле привязано к ограниченному пространству и группе индивидуумов. Оно влечёт за собой преимущества, права и обязанности. Цифровое гражданство — это знание правил надлежащего ответственного поведения и применения технологий во всех аспектах повседневной жизни и деятельности. Это участие в сетевых сообществах, и умение использовать Интернет с позиций здравого смысла, не нанося при этом ущерба любого рода другим пользователям и вдохновляя их делать то же самое. Но особенным его делает тот факт, что оно приносит гораздо больше соотечественников: порядка трёх миллиардов человек⁸.

Цифровое гражданство поднимает дополнительно ряд других вопросов, а именно, обязательный баланс между преимуществами, которые дают технологии, и потенциальными рисками, например, такими, как недопустимый контент и кибербуллинг, этические проблемы, такие, как авторское право и плагиат. По утверждению доктора Майка Риббла, разработчика

⁶ Jason Ohler, @Character education for the digital age» Te@chThought (blog), May 2, 2013. Режим доступа: <http://teachthought.com/technology/the-definition-of-digital-citizenship/> (Последнее посещение 10.10.2017)

⁷ Ribble, Mike, and Gerald Bailey. Digital Citizenship in Schools. Eugene: ISTE, 2007. E-book.

⁸ Terry Heick, «The definition of digital citizenship» Te@chThought (blog), May 2, 2013. Режим доступа: <http://teachthought.com/technology/the-definition-of-digital-citizenship/> (Последнее посещение 10.10.2017).

концепции, «цифровое гражданство, — это больше, чем просто учебный инструмент, это способ подготовки учащихся к жизни в обществе, насыщенном технологиями»⁹. Следует подчеркнуть, что подход цифрового гражданства принят в ряде штатов США и Канады.

Говоря о международном подходе, Международное Общество Технологий в Образовании (ISTE) сформировало перечень стандартов для учащихся, преподавателей, и школьной администрации, описывающих технологические навыки, которые необходимо освоить учащимся. Перечень стандартов для учащихся, среди прочих вещей, включает обучение цифровому гражданству¹⁰.

Таким образом, формирование у учащихся навыков цифрового гражданства чрезвычайно важно. Разработчики концепции определили 9 элементов гражданства. Рассмотрим эти элементы более подробно.

1. Цифровой доступ: пропаганда равных цифровых прав и доступа — это начало цифрового гражданства. Цифровой доступ относится к способности всех учащихся принимать активное участие в цифровом сообществе. В этой ситуации негативное влияние могут оказать социально-экономический статус (материальное положение семьи учащегося), местоположение (проживание в удалённом районе). Таким образом, школы должны учитывать, все ли учащиеся имеют доступ к электронным устройствам и подключены к Интернету

2. Цифровой этикет: правил и политик недостаточно; разработчики настаивают, что всех нужно учить правилам поведения в Интернете. Цифровой этикет описывает стандарты поведения в онлайн-пространстве или при использовании технологий. Такие правила зачастую не описаны; к тому же они быстро меняются, поскольку появляются новые технологии, и они могут варьироваться от одной группы пользо-

вателей к другой. У разных поколений взгляды также могут расходиться по поводу того, что считается вежливым, например, пользование мобильным телефоном во время личной беседы. Хотя базовым правилам этикета в первую очередь родители учат детей, они нередко не знают, что считается нормальным поведением в цифровых сетях, и учатся вместе с детьми. Поэтому крайне важно, чтобы школа играла ключевую роль в обучении цифровому этикету как части учебной программы.

3. Цифровое право. Крайне важно, чтобы пользователи понимали, что украть или повредить чужую цифровую работу, нанести ущерб личности или собственности — это нарушение закона. Законодательное регулирование включает такие вопросы, как обмен или использование материалов под защитой авторского права, кража идентичности.

Молодёжь гораздо менее склонна воспринимать некоторые потенциально незаконные действия, как, например, скачивание музыки или видео, как незаконные или неэтичные; на самом деле 46% учащихся считают, что незаконное скачивание контента не имеет большого значения, и чем старше учащиеся, тем этот показатель выше¹¹. А зачастую они просто не знают о юридических последствиях. Они также не знают о лицензии Creative Commons, регулирующей использование чужого материала. Отношение молодёжи к этике и законности стало особенно проблематичным в ситуации с секстингом, когда происходил обмен обнажёнными или полуобнажёнными фотографиями. В некоторых странах, таких, как Великобритания, Канада, отдельные

⁹ Ribble, Mike, and Gerald Bailey. *Digital Citizenship in Schools*. Eugene: ISTE, 2007. E-book.

¹⁰ International Society for Technology in Education. *ISTE Standards: Students*. International Society for Technology in Education: 2007. Режим доступа: http://www.iste.org/docs/pdfs/20-14_ISTE_Standards-S_PDF.pdf (Последнее посещение 10.10.2017).

¹¹ Steeves, Valerie. *Young Canadians in a Wired World, Phase III: Experts or Amateurs? Gauging Young Canadians' digital literacy skills*. Ottawa: Media Smarts, 2014. Режим доступа: http://mediasmarts.ca/sites/default/files/pdfs/publication-report/full/YSWWIII_Experts_or_Amateurs.pdf (Последнее посещение 10.10.2017).

штаты США отсылка детской обнажённой фотографии приравнена к распространению детской порнографии даже если на фотографии изображён сам отправитель. В связи с тем, что технологии постоянно развиваются, очень сложно тщательно проработать регулирующие законодательные нормы, и очень важно, чтобы и школьная администрация, и учителя были в курсе происходящих изменений в законодательстве и старались регулировать занятия учащихся в Интернете с учётом существующих законодательных норм¹².

4. Цифровая связь. Имея так много доступных коммуникационных возможностей, пользователям необходимо научиться принимать правильные решения.

Цифровая связь включает любую электронную среду, посредством которой люди общаются, например, мобильные телефоны, социальные сети, электронную почту и текстовые сообщения. Вездесущность цифровой связи может создать проблемы во время проведения уроков, когда учителям может показаться, что сотовые телефоны, планшеты или компьютеры на уроке приведут к недостатку или нежелательному отвлечению внимания, например, возможными телефонными звонками, обменом смс-сообщениями или электронной почтой, не связанными с содержанием урока. Это нередко приводит, например, к запретам сотовых телефонов на уроках.

5. Цифровая грамотность: необходимо научить учащихся, как учиться в цифровом обществе. Цифровая грамотность предполагает процесс обучения надлежащему использованию технологий. Даже когда технология часто используется на уроках, учащиеся зачастую не владеют навыками цифровой грамотности, в то время как по умолчанию предполагается, что они уже обладают этими навыками. Однако, хотя учащиеся являются активными пользователями технологий,

они по-прежнему нуждаются в инструкциях по надлежащему использованию.

Цифровая грамотность включает такие навыки, как поиск информации, оценка содержания веб-сайтов, сотрудничество в сетях и умение «просеивать» большое количество информации, доступной онлайн. Для того, чтобы формировать эти навыки у учащихся, учителя должны сначала сами их освоить, а затем моделировать ситуации на уроках с тем, чтобы впоследствии учащиеся смогли их применять в контекстах реального мира.

6. Цифровая торговля. Цифровая торговля — это покупка и продажа товаров через Интернет. Поскольку пользователи делают всё больше покупок в Интернете, они должны понимать, как быть грамотными покупателями в условиях цифровой экономики.

Хотя может показаться, что этот элемент цифрового гражданства не имеет прямого отношения к школе, следует признать, что учащиеся всё чаще совершают онлайн-покупки. Harris Interactive обнаружил, что американцы в возрасте 8–24 лет в 2009 году потратили 220 миллиардов долларов, делая покупки онлайн¹³. Кроме того, быть информированным потребителем — это важный аспект цифрового гражданства, и поэтому на школах лежит ответственность за освещение этого аспекта на занятиях. Учащихся нужно научить принимать обдуманные решения, делая покупки онлайн, чтобы не стать жертвой мошенничества.

7. Цифровые права и обязанности: Гражданство в любом сообществе имеет привилегии и обязанности, и цифровые сообщества ничем не отличаются. Цифровые права включают, прежде всего, право на доступ к Интернету; они также включают возможность размещать контент онлайн без его кражи или плагиата и возможность участия в онлайн-сетях, не опа-

¹² Богданова Д.А. Ещё раз о медиаграмотности и интернет-безопасности // Дистанционное и виртуальное обучение. — 2016. — № 5. — С. 74–82.

¹³ Ribble, Mike. Digital Citizenship in Schools. Washington, D.C.: ISTE, 2011. Kindle edition.

саясь запугивания или преследования. Цифровые обязанности включают требование следовать существующему цифровому праву и использовать технологию ответственно и этически (например, указание соответствующей ссылки при использовании онлайн-источников, а не использование технологий для выполнения задания на основе обмана или подлога).

8. Цифровая безопасность: цифровые граждане должны знать, как защитить личную информацию от внешнего вмешательства, которое может причинить вред, нанести ущерб. Цифровая безопасность относится к стратегиям и мерам предосторожности, которые должны предпринимать отдельные лица для обеспечения их безопасности от вирусов, взломов. В контексте школы проблема состоит в неумении учащихся адекватно защищать персональные данные, а слабые пароли или их совместное использование могут поставить школьную сеть под угрозу заражения вирусами или взлома. Поэтому на школы ложится обязанность научить учащихся знаниям о фишинговых атаках, необходимости использовать сильные пароли (а не делиться ими, даже с доверенными друзьями), регулярно обновлять антивирусную защиту на устройствах и создавать резервные копии материалов.

9. Цифровое здоровье и благополучие. Учащиеся должны понимать риски для здоровья от чрезмерного использования технологий, таких, например, как синдром постоянного стресса, и о психологических проблемах, таких как интернет-зависимость. Цифровое здоровье и благополучие включает как физические, так и психологические аспекты. Физические аспекты могут включать потенциальные риски для здоровья от чрезмерного использования технологий, таких как синдром кистевого туннеля, синдром блэкбэри, зрительный стресс и плохая осанка¹⁴. Физические последствия также могут быть следствием недостатка двигательной активности, когда учащиеся тратят слишком мно-

¹⁴ Богданова Д.А., Федосеев А.А. Современные особенности клавиатурного ввода // Дистанционное и виртуальное обучение. 2015. — №12. — С. 104–113.

го времени на занятия в сидячем положении. Психологические проблемы могут возникать из-за чрезмерного использования технологий¹⁵. Например, недавние зарубежные исследования показали, что продолжительное время, проведённое в Facebook, коррелирует со снижением восприятия личного благополучия и удовлетворённости жизнью¹⁶. Эти исследования свидетельствуют о необходимости умеренности и самоконтроля во время пребывания онлайн.

Цифровое гражданство — сложная тема со многими аспектами. Мы должны убедиться, что помогаем учащимся понять проблемы, которые могут возникнуть в Интернете, подчёркивая при этом позитивное влияние технологий. Как известно многим педагогам, большинство учащихся хотят поступать правильно, если они знают, как это делать. Следует помогать им делать хорошие вещи, используя технологии и избегая при этом ошибок. Поэтому следует подчеркнуть, что совместная инновационная деятельность Федерального центра «Информатика и управление» Российской академии наук с Архангельским областным институтом открытого образования в рамках проекта «Безопасное использование возможностей электронного обучения в общеобразовательных организациях» отвечает веяниям времени. Этот проект посвящён формированию культуры безопасного использования компьютерного оборудования и ресурсов сети Интернет учащимися общеобразовательных организаций. **НО**

¹⁵ Ribble, Mike. Digital Citizenship in Schools. Washington, D.C.: ISTE, 2011. Kindle edition.

¹⁶ Ethan Cros et al. Facebook Use Predicts Declines in Subjective Well-being in young adults Plos One (2013). Режим доступа: <http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0069841> (Последнее посещение 10.10.2017).