Защита детей и подростков от киберугроз: что могут родители?

Калинина Т.В.
Московский педагогический государственный
университет (МПГУ), г. Москва, Российская Федерация
ORCID: https://orcid.org/0000-0002-4896-2394
e-mail: t.kalinina@bk.ru

Статья посвящена вопросам защиты детей и подростков от существующих киберугроз. Рассмотрены виды киберугроз с которыми могут встретиться дети, как пользователи Интернет и социальных сетей. Предложены способы противодействия распространенным киберугрозам, реализовать которые смогут родители, независимо от уровня цифровой компетентности.

Ключевые слова: киберугрозы информационного пространства; киберзащита детей; кибербезопасность; безопасный интернет; цифровая безопасность.

Для цитаты:
Калинина Т.В. Защита детей и подростков от киберугроз: что могут родители? // Цифровая гуманитаристика и технологии в образовании (DHTE 2021): сб. статей II Всероссийской научно-практической конференции с международным участием. 11–12 ноября 2021 г. / Под ред. В.В. Рубцова, М.Г. Сороковой, Н.П. Радчиковой. М.: Издательство ФГБОУ ВО МГППУ, 2021. 488–497 с.

Стереотип о том, что большинство современных детей предпочитают школе, спортивным секциям и общению со сверстниками компьютерные игры уже утратил свою актуальность. В портрете современного ребенка все больше место занимает сегмент «Ребенок – медиапотребитель». Данные последних масштабных исследований свидетельствуют, что в России дети являются самой многочисленной частью социума. 22,6 миллионов детской аудитории по медиапотребелнию значительно опережают даже подростков. Согласно данным, детская аудитория проявляет интерес к различному контенту: телевидение – 72 %; игры – 71 %; музыкальный сегмент 42 % и по-прежнему лидирует печатная продукция – 77 %.

В конце 2019 года были опубликованы результаты аналитического проекта «Детский рунет». Результаты проведенной серии исследований ошеломляют: Интернетом в России пользуются более 93 % детей от 5 до 11 лет – это почти 5 миллионов детей. Из возрастной категории от 5 до 7 лет пользуются всемирной паутиной 89 % –

это 2,1 миллион детей. Среди детской аудитории от 8 до 11 лет – 97 %, т.е. 2,74 миллиона детей.

Показательно, что с течением времени дети все раньше начинают пользоваться интернетом. Пользователи в возрасте 8–11 лет начинают выходить в Сеть в 6–7 лет, а 5–7-летние – в 4–5 лет. При этом более трети представителей младшей возрастной группы пользуются интернетом самостоятельно, а к 8–11 годам этот показатель возрастает до 55 %.

Смартфон явился самым распространенным устройством для выхода детей в Интернет. 67 % детей от 5 до 11 лет и 74 % детей от 8 до 11 лет используют смартфон. Доступ к сети с помощью планшета привлекает более молодую часть респондентов – от 5 до 7 лет. Посещают интернет с помощью ноутбука и стационарного компьютера дети более старшего возраста. В этой категории процент пользователей увеличивается до 40 %.

Родители поддерживают стремление детей и предоставляют доступ к медиаконтенту. Больше половины детей (59 %) до 12 лет могут ежедневно пользоваться смартфоном или планшетом родителей. Собственные цифровые устройства, включая мобильные телефоны начинают появляться у детей в возрасте до 3-х лет. Собственным гаджетом владеет каждый 10-й ребенок. Из возрастной категории детей от 4 до 7 лет – планшеты имеет 24 %; смартфон – 16 %. 9 из 10 Российских детей к своим десяти годам получают телефон или планшет, либо сразу оба устройства [2; 3].

С одной стороны – эти тенденции связаны с развитием технологий и появлением нового поколения родителей, которые пользуются интернетом с детства. С другой такая статистика обозначает стойкий интерес детей к Интернет-ресурсам, который усиливается с взрослением ребенка. В этой связи актуальным становится вопрос защиты детей от опасностей, с которыми ребенок может столкнуться.

Среди опасностей Интернета, обозначенных родителями на первом месте – порнография и эротика в Интернете, на втором – пропаганда суицида, на третьем – жестокость и агрессия, на четвертом – ненужная или не соответствующая возрасту информация. Безусловно, имея доступ к средствам ИКТ и современным возможностям сети, дети получают огромное количество информации самого разного содержания.

На государственном уровне проблема обеспечения информационной безопасности детей регулируется документами: Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» [6] и «Концепция информационной безопасности детей» [5]. Информационная безопасность в этих докумен-

тах трактуется, как «...состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию». В данных документах четко выражена мысль о том, что: «...обеспечение информационной безопасности детей возможно исключительно при условии эффективного сочетания государственных и общественных усилий при определяющей роли семьи». Следовательно, на взрослых лежит обязанность обеспечения духовной и психологической защиты ребенка от деструктивной информации современной информационной среды.

Вместе с тем, родители, психологи и педагоги все больше обеспокоены негативным влиянием средств массовой информации (СМИ), телевидения, социальных сетей, Интернета и цифровой развлекательной индустрии на психику, физическое и духовно-нравственное развитие детей и подростков.

Специалисты предупреждают: постоянное воздействие негативных факторов современной цифровой среды в конечном счете могут привести к снижению уровня психологической и личностной зрелости ребенка. Отмечают опасность задержки развития сферы воображения, при восприятии информации выраженную ориентацию на наглядность. Вызывает опасение формирование коммуникативных умений и навыков, слабость произвольной сферы и искажение восприятия мироустройства. К факторам риска также относятся и киберугрозы, с которыми дети встречаются в цифровом пространстве.

Примечательно то, что никто из практиков области образования не призывает родителей отказываться от СМИ, телевидения, категорически исключить компьютерно-игровую деятельность и прятать средства информационных коммуникационных технологий, приходя домой с работы! Маловероятно, что удастся создать подобную «стерильную» среду для современного ребенка на протяжении какого-либо времени. Да и в плане развития и соответствия реалиям общества такой подход сложно назвать верным. Но и пренебрежение со стороны взрослых вопросами информационной безопасности может принести ощутимый вред психологическому и физическому здоровью ребенка. Не стоит закрывать глаза и обесценивать опасность, исходящую от вещей, уже ставших повседневной реальностью говоря, что у всех такие же проблемы и остальные как-то справляются с ними, перерастают и т.д.

В целом, последствия неуправляемого и необдуманного взаимодействия детей с цифровым миром можно разделить на несколько категорий:

1. Негативное влияние на психику ребенка. Самые распространенные жалобы этой категории: эмоциональная неустойчи-

вость; агрессивное поведение ребенка; снижение самооценки; развитие компьютерной зависимости; отказ от других видов деятельности и др.
2. Ухудшение физического здоровья ребенка: ухудшение зрения; нарушения опорно-двигательного аппарата и осанки; головные боли; трудность с засыпанием и др.
3. Социальная дезадаптация личности: трудности в установлении взаимоотношений со сверстниками; напряженность отношений с родителями и взрослыми; снижение качества формирования навыков учебной деятельности; появление антисоциального поведения и др.
4. Угроза жизни ребенка от преступников. В цифровом пространстве сложно узнать с кем ребенок общается. Преступники создают профиль, в котором представляют себя как сверстника и начинают общаться с ребенком на увлекательные темы. Встречается информация о том, что за 1,5 часа опытный преступник вполне в состоянии уговорить ребенка встретиться с ним в реальности.

Предположу, что точное знание того, как действовать в опасной ситуации, дает некоторую уверенность в том, что ребенок защищен. Рассмотрим какие киберугрозы, с которыми встречаются дети, как пользователи Интернета и различных социальных сетей могут быть опасными:

Нежелательный контент. К нежелательному контенту относится все то, о чем ребенку не следовало бы узнавать, как можно долгое время. К этой категории относятся порносайты, информация, пропагандирующая агрессивное поведение, алкоголизм, употребление наркотиков, самоубийство и многое другое. Нежелательный контент самая частая угроза, с которой сталкиваются дети в интернет-пространстве. При этом дети редко делятся с родителями своими открытиями.

Развитие пристрастия к азартным играм. Вопреки мнению, что дети сами «перерастут» игровую зависимость, это случается довольно редко. Чаще всего одни игры сменяются другими. Времени и потребности заниматься чем-либо еще становится все меньше. Более того, в современных играх часто предлагают купить некоторые опции за деньги.

Кибербуллинг, или онлайн-травля. Это угроза, с которой многие дети сталкиваются начиная со школьного возраста. На личный аккаунт или телефон ребенка приходят сообщения с угрозами и оскорблениями. В социальных сетях, к которым есть доступ и у пострадавшего ребенка размещаются призывы к его бойкотированию

или печатаются сплетни, порочащие ребенка. Практика показывает, что большинство детей, подвергающихся онлайн-травле сверстников пытается пережить этот момент самостоятельно, стесняясь обратиться за помощью к взрослым.

К различным видам мошенничества относятся фишинг (у детей пытаются разными способами узнать конфиденциальную информацию, номера и пароли банковских карт родителей и т.д.). Выглядеть данный вид мошенничества может как сообщение о том, что необходимо подтвердить личную информацию на псевдо сайте и тогда станет доступен крупный выигрыш, денежное вознаграждение, телефон новой модели и многое другое.

Непреднамеренная трата денег относится к угрозам, с которыми сталкиваются не только дети и подростки, но и взрослые. Украсть деньги могут, предложив перейти по ссылке, либо просят ввести номер телефона, отправить СМС. В последнее время способы отъёма денег все более совершенствуются. Преступники могут позвонить лично с просьбой вернуть якобы перечисленные вам по ошибке деньги. Может прийти СМС от «друга», который попал в беду и отчаянно нуждается в помощи и т.д. Списание денег с вашего счета может происходить и легально. Во многих бесплатных онлайн-играх игрокам предлагается купить за деньги различные опции, дающие ощутимые преимущества в игре.

Вирусные атаки. Вредоносность вирусов знакома всем. Однако многие все равно скачивают непроверенные файлы. В результате заражения вирусом ваш компьютер может сломаться и потребуется дорогостоящий ремонт. С помощью вирусов осуществляется кража конфиденциальной информации, личная переписка и многое другое, что в последствии может служить для преступников предметом шантажа.

Доступ к личной информации. Необходимо знать, что ваша домашняя сеть не безопасна. Любая информация, которую вы размещаете или ищете, доступна любому. Особенно осторожно следует относиться к той информации, которую Вы размещаете в социальных сетях. В школьном возрасте дети очень активно начинают самостоятельно пользоваться социальными сетями. Девочки, например очень любят размещать свои личные фотографии (что одела, что ела, как причесалась, интерьеры дома и т. д). Обязательно надо говорить детям о том, что любую их фотографию и размещенную информацию сможет увидеть любой человек, даже проходящий по улице мимо незнакомец.

Кибергруминг – это прямая угроза жизни и здоровью детей от незнакомцев, предлагающих личные встречи. Общаясь в социальной

сети с ребенком, преступник устанавливает эмоциональную связь с целью сексуального насилия и/или убийства. Согласно данным сайта Kaspersky («Лаборатория Касперского»), «...больше половины детей в возрасте 7–18 лет получали в сети приглашение «дружить» от незнакомых людей, в 34 % случаев это были взрослые. Более того, к каждому девятому ребёнку в возрасте 11–14 лет незнакомцы уже пытались «втереться в доверие». А каждый третий школьник даже встречался с людьми, с которыми познакомился в соцсетях...» [4].

Каким образом можно помочь детям избежать негативных последствий общения с современной информационной средой, не обладая при этом высоким уровнем цифровой грамотности? Во-первых, нужно понимать, что невозможно полностью оградить ребенка от столкновения с нежелательным контентом и опасностями цифрового пространства. Более продуктивным будет информирование детей о существующих киберугрозах, разработка совместно с ребенком мер противодействия, которые он в силах реализовать самостоятельно. Поможет также правило – в спорных ситуациях необходимо обращаться за помощью к взрослым!

Во-вторых, существует несколько правил кибербезопасности, выполнять которые нужно взрослым неукоснительно. А некоторые из них должны знать дети:

1. Ограничить время провождения в сети. Не путем запрета, а путем заинтересованности другими видами деятельности. Отлично справляются с этой задачей секции, хобби, интересы, не связанные с цифровым пространством и т.д. Даже если интерес ребенка все равно находится в области цифровых технологий, можно перевести его на продуктивный, познавательный и развивающий уровень. Многие профессии будущего связаны с цифровыми облачными технологиями.
2. Использовать средства обеспечения безопасности в интернет-пространстве. Это могут быть фильтры Интернет-содержимого (Windows Vista, Windows Live и др.) или бесплатная программа «Интернет Цензор». Позаботьтесь об установке антивирусной программы. Можно подключить у провайдера услугу «Детский Интернет». С помощью функции «Родительский контроль» можно регулировать использование компьютера детьми.
3. Познакомить ребенка с существующей маркировкой по возрасту (0+, 6+, 12+, 16+, 18+). Следить, чтобы при выборе программ или фильмов эта маркировка ребенком соблюдалась.
4. Объяснять детям, что нельзя принимать за правду все то, что пишут в Интернете. Познакомить ребенка с существующими опасностями «всемирной паутины». Правду жизни следует соотносить с возрастом ребенка.

5. Убедить ребёнка не указывать своё реальное имя и фамилию при регистрации. Безопасней, если без взрослых ребенок вообще не будет регистрироваться даже на безобидных, первый взгляд сайтах. Требование о введении личных данных (ребенку надлежит знать, что к ним относят) должно насторожить и служить поводом обращения к взрослому.
6. Взять себе за правило периодически просматривать подписчиков ребёнка в соцсетях. Обращать внимание следует на незнакомых ребят, взрослых людей и т.д. Для этого подпишитесь на страничку своего ребенка в соцсетях.
7. Объяснить, что соглашаться на встречу с онлайн-друзьями небезопасно.
8. Быть внимательными к ребёнку. Важно не пропустить признаки интернет-буллинга. Продолжительное ухудшение настроения, отказ общаться с друзьями, добровольное затворничество, резкое удаление из подписок друзей должны насторожить родителей.
9. Стараться проводить как можно больше совместного времени с ребенком. В любой ситуации ребенок должен быть уверен, что его выслушают и поддержат. Старайтесь вместе читать, смотреть фильмы и рассуждать над увиденным и прочитанным.
10. Рассказать, что нельзя проходить по незнакомым ссылкам и скачивать файлы, в большом количестве рассылаемых по сетям.
11. Избегать личного использования Интернет-пространства ребенком до 7 лет. В 2020 году утвержден официальный документ «Гигиенические нормативы и специальные требования к устройству, содержанию и режимам работы в условиях цифровой образовательной среды в сфере общего образования» [1]. В этом документе четко обозначены временные нормативы использования средств ИКТ в школе и дома для 1–11 классов.
12. Родителям необходимо взвесить все за и против, прежде чем размещать в аккаунте фотографии и видео своих детей. Аккаунты взрослых являются не менее широкой базой для мошенников.
13. Читать специальную литературу, посвященную вопросам информационной безопасности (и детям, и взрослым). В интернете появились многочисленные видео ролики данной тематики, которые будет интересно и познавательно посмотреть вместе с ребенком.

Литература

1. Гигиенические нормативы и специальные требования к устройству, содержанию и режимам работы в условиях цифровой образовательной среды в сфере общего образования. [Электронный ресурс] // Руководство. М.: НМИЦ здоровья детей Минздра-

ва России, 2020. 20 с. URL: https://548-parents.ru/wp-content/uploads/2020/09/Normativi.pdf (дата обращения: 11.09.2021).
2. Дети и интернет: аналитический отчет. [Электронный ресурс] // Доклад по исследованиям компании Mediascope, сервиса по аналитике соцсетей Brand Analytics и фонда «Общественное мнение». URL: https://activityedu.ru/Blogs/analytics/deti-v-runete-analiticheskiy-otchet/ (дата обращения: 11.09.2021).
3. Дети. Медиапотребление. 2017. [Электронный ресурс] // Отчет MOMRI. URL: https://cyberpsy.ru/articles/children_media_2017_momri/ (дата обращения: 11.09.2021).
4. Кибербуллинг. [Электронный ресурс] // Итоги опроса «Лаборатории Касперского» URL: https://www.kaspersky.ru/about/press-releases/2019_ksk-survey (дата обращения: 15.09.2021).
5. Концепция информационной безопасности детей (Утверждена распоряжением Правительства РФ от 2 декабря 2015 года N 2471-р. [Электронный ресурс] // Сайт Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_190009/65c73cdecf9794a8f8f67bdb438d964c9336f436/ (дата обращения: 11.09.2021).
6. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 N 436-ФЗ (ред. от 31.07.2020) [Электронный ресурс] // Сайт Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_108808/ (дата обращения: 11.09.2021).

Информация об авторе

Калинина Татьяна Валерьевна, кандидат педагогических наук, старший преподаватель кафедры дошкольной педагогики Факультет дошкольной педагогики и психологии, Московский педагогический государственный университет (МПГУ), г. Москва, Российская Федерация ORCID: https://orcid.org/0000-0002-4896-2394, e-mail: t.kalinina@bk.ru

Protecting children and adolescents from cyber threats: what can parents do?

Tatiana V. Kalinina
Moscow Pedagogical State University, Moscow, Russia
ORCID: https://orcid.org/0000-0002-4896-2394
e-mail: t.kalinina@bk.ru

The article is devoted to the protection of children and adolescents from existing cyber threats. The types of cyber threats that children can encounter, as users of the Internet and social networks, are considered. The methods of countering common cyber threats are proposed, which parents will be able to implement, regardless of the level of digital competence.

Keywords: cyber threats of the information space; cyber protection of children; cybersecurity; secure Internet; digital security.

For citation:
Kalinina T.V. Protecting children and adolescents from cyber threats: what can parents do? // Digital Humanities and Technology in Education (DHTE 2021): Collection of Articles of the II All-Russian Scientific and Practical Conference with International Participation. November 11–12, 2021 / V.V. Rubtsov, M.G. Sorokova, N.P. Radchikova (Eds). Moscow: Publishing house MSUPE, 2021. 488–497 p.

References

1. Gigienicheskie normativy i spetsial'nye trebovaniya k ustroistvu, soderzhaniyu i rezhimam raboty v usloviyakh tsifrovoi obrazovatel'noi sredy v sfere obshchego obrazovaniya. [Elektronnyi resurs] // Rukovodstvo. M.: NMITs zdorov'ya detei Minzdrava Rossii, 2020. 20 p. URL: https://548-parents.ru/wp-content/uploads/2020/09/Normativi.pdf (data obrashcheniya: 11.09.2021).
2. Deti i internet: analiticheskii otchet. [Elektronnyi resurs] // Doklad po issledovaniyam kompanii Mediascope, servisa po analitike sotssetei Brand Analytics i fonda «Obshchestvennoe mnenie». URL: https://activityedu.ru/Blogs/analytics/deti-v-runete-analiticheskiy-otchet/ (data obrashcheniya: 11.09.2021).
3. Deti. Mediapotreblenie. 2017. [Elektronnyi resurs] // Otchet MOMRI. URL: https://cyberpsy.ru/articles/children_media_2017_momri/ (data obrashcheniya: 11.09.2021).
4. Kiberbulling. [Elektronnyi resurs] // Itogi oprosa «Laboratorii Kasperskogo» URL: https://www.kaspersky.ru/about/press-releases/2019_ksk-survey (data obrashcheniya: 15.09.2021).
5. Kontseptsiya informatsionnoi bezopasnosti detei (Utverzhdena rasporyazheniem Pravitel'stva RF ot 2 dekabrya 2015 goda N 2471-r. [Elektronnyi resurs] // Sait Konsul'tant Plyus. URL: http://www.

consultant.ru/document/cons_doc_LAW_190009/65c73cdecf9794a8f8f67bdb438d964c9336f436/ (data obrashcheniya: 11.09.2021).
6. Federal'nyi zakon «O zashchite detei ot informatsii, prichinyayushchei vred ikh zdorov'yu i razvitiyu» ot 29.12.2010 N 436-FZ (red. ot 31.07.2020) [Elektronnyi resurs] // Sait Konsul'tant Plyus. URL: http://www.consultant.ru/document/cons_doc_LAW_108808/ (data obrashcheniya: 11.09.2021).

Information about the authors

Tatiana V. Kalinina, Candidate of Pedagogical Sciences, Senior Lecturer of the Department of Preschool Pedagogy, Moscow Pedagogical State University, Moscow, Russian Federation, e-mail: t.kalinina@bk.ru