Психологическая наука и образование
2021. Т. 26. № 4. С. 43—53
DOI: https://doi.org/10.17759/pse.2021260404
ISSN: 1814-2052
ISSN: 2311-7273 (online)

Psychological Science and Education
2021. Vol. 26, no. 4, pp. 43—53
DOI: https://doi.org/10.17759/pse.2021260404
ISSN: 1814-2052
ISSN: 2311-7273 (online)

# Как российские школьники противостоят киберугрозам?

***Скобельцина К.Н.***
ФГБНУ «Институт управления образованием Российской академии образования» (ФГБНУ ИУО РАО), г. Москва, Российская Федерация
ORCID: https://orcid.org/0000-0003-0673-7620, e-mail: skobeltsina@iuorao.ru

***Кузнецов А.Н.***
ФГБНУ «Институт управления образованием Российской академии образования» (ФГБНУ ИУО РАО), г. Москва, Российская Федерация
ORCID: https://orcid.org/0000-0003-1573-5491, e-mail: kuznetsov@iuorao.ru

***Бешенков С.А.***
ФГБНУ «Институт управления образованием Российской академии образования» (ФГБНУ ИУО РАО), г. Москва, Российская Федерация
ORCID: https://orcid.org/0000-0001-7225-5924, e-mail: srg57@mail.ru

Рассматриваются особенности поведения российских школьников, сталкивающихся с новым социальным и психологическим феноменом — угрозами в цифровой среде. В фокусе внимания исследователей — способность и техническая готовность подростка противостоять киберугрозам. На подготовительном этапе исследования авторами проведен анализ российского и международного опыта изучения проблематики обеспечения подготовленности школьников к противостоянию киберугрозам, в том числе с учетом нового социального контекста, появление которого определено распространением коронавирусной инфекции. В качестве основного метода исследования использован социологический опрос на основе авторской анкеты, в котором осенью 2020 г. приняли участие подростки — обучающиеся 7—11 классов общеобразовательных школ из семи регионов России (N=5682). Материалы исследования обрабатывались с помощью математико-статистических программ SPSS и STATISTICA. В качестве основных результатов можно выделить диагностику уровня владения школьниками методами и средствами защиты личной информации, а также их способности противодействовать цифровым угрозам на уровне знаний и умений. Определена роль школы в формировании готовности школьников к реалиям современного цифрового мира. Выявлены типичные дефициты в цифровой компетентности школьников, прежде всего в сфере знания о типах рисков, связанных с использованием информационно-коммуникативных сетей. Делается вывод о принятии системных управленческих решений на разных уровнях системы образования, направленных на снижение киберрисков при использовании подростками социальных сетей и повышение качества развития цифровых компетенций в российских школах.

***Ключевые слова:*** цифровизация детства, кибербезопасность, киберугрозы, дети в интернете, цифровые навыки, киберриски.

**Финансирование.** Исследование выполнено в рамках исполнения государственного задания ФГБНУ «Институт управления образованием Российской академии образования» при финансовой поддержке Министерства просвещения Российской Федерации.

**Благодарности.** Авторы благодарят за помощь в сборе данных для исследования коллектив Института управления образованием Российской академии образования.

**Для цитаты:** *Скобельцина К.Н., Кузнецов А.Н., Бешенков С.А.* Как российские школьники противостоят киберугрозам? // Психологическая наука и образование. 2021. Том 26. № 4. С. 43—53. DOI: https://doi.org/10.17759/pse.2021260404

# Russian Schoolchildren vs. Cyber Threats: Research in the Framework of Modern Childhood Digitalization

***Ksenia N. Skobeltsina***
Institute of Education Management of the Russian Academy of Education, Moscow, Russia
ORCID: https://orcid.org/0000-0003-0673-7620, e-mail: skobeltsina@iuorao.ru

***Andrei N. Kuznetsov***
Institute of Education Management of the Russian Academy of Education, Moscow, Russia
ORCID: https://orcid.org/0000-0003-1573-5491, e-mail: kuznetsov@iuorao.ru

***Sergey A. Beshenkov***
Institute of Education Management of the Russian Academy of Education, Moscow, Russia
ORCID: https://orcid.org/0000-0001-7225-5924, e-mail: srg57@mail.ru

The paper aims to explore the behavior of Russian school-age children who are faced with a new social and psychological phenomenon: threats associated with the digital environment. Our focus was on the ability (psychological as well as technical) of teenagers to stand against cyber threats. At the preliminary stage of the research we analysed both Russian and international studies on how to promote cyber security awareness among school children and, in particular, how to respond to the cyber threats associated with the new social context formed by the COVID-19 pandemic. We used survey research as the main method and designed a special questionnaire that was then offered to a group of 7—11-grade students (N=5,682) from seven Russian regions in the late 2020. The research data was processed using the SPSS and STATISTICA programmes. The data allowed us to assess the degree in which the children were familiar with the methods and means of protecting sensitive personal information, as well as their ability to stand against cyber threats basing on their knowledge and skills. The research also helped us to identify the role of schools in promoting the children's readiness for the modern digital reality. The typical shortcomings in the digital competences of school-age children are noteworthy here too, first of all, the ones concerning the knowledge of cyber risk types related to the use of social media and internet communication services. We conclude that there is a need for systemic measures on various levels of education that would help reduce the cyber risks for adolescents on the social media and promote the quality of digital competence development in Russian schools.

***Keywords:*** digitalization of childhood, E-safety, cyberbullying, children on the Internet, digital skills, cyber risks.

**Funding.** This paper was prepared as part of the state project of the Federal State Budgetary Scientific Institution «Institute of Education Management of the Russian Academy of Education» with financial support from the Ministry of Education of the Russian Federation.

**Acknowledgements.** The authors are grateful to the staff of the Institute of Education Management of the Russian Academy of Education for their assistance in data collection.

**For citation:** Skobeltsina K.N., Kuznetsov A.N., Beshenkov S.A. Russian Schoolchildren vs. Cyber Threats: Research in the Framework of Modern Childhood Digitalization. *Psikhologicheskaya nauka i obrazovanie = Psychological Science and Education*, 2021. Vol. 26, no. 4, pp. 43—53. DOI: https://doi.org/10.17759/pse.2021260404 (In Russ.).

## Введение

В последнее время в мировой и российской информационной сфере произошли значительные изменения. Спектр информационных угроз — потенциально возможных событий, которые могут привести к нанесению ущерба информационной безопасности — существенно расширился и качественно изменился. Педагоги и руководители систем образования сегодня должны учитывать в своей работе такие киберугрозы, как фишинг, троллинг, кибербуллинг, развитие социальных сетей (в том числе активизация в них деятельности сект и экстремистских, преступных сообществ), расширение доступности и привлекательности онлайн-игр и др. [8; 17]. При этом очевидно, что необходимым условием для внедрения и функционирования цифровой образовательной среды является информационная безопасность —— «состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию» [6].

Кибербезопасность, то есть способность человека эффективно реагировать на вызовы и возможности, предлагаемые интернетом, является важным навыком, которому необходимо обучать детей с раннего возраста как в семье, так и в системе образования [15; 16]. Вопросы, связанные со школьным кибербуллингом, поднимаются рядом экспертов в области образования в разных регионах [9; 12; 13; 16; 22]. Исследователи выявляют развитие таких феноменов, как киберчеловеческие ценности, киберчерты характера, кибервиктимизация, кибервмешательство и др., исследуют выражение подростками суицидальных намерений в социальных сетях и т.д. Исследования (в частности, проведенные нами ранее) показывают, что более 30% школьников сталкивались с кибербуллингом и личным вмешательством со стороны незнакомцев в интернете, при этом большинство учащихся, ставших жертвами кибербуллинга (более 60%), не обращаются за помощью, пытаясь справиться с атакой самостоятельно [9; 21].

Международные авторы описывают положительный опыт запуска специальных обучающих программ, направленных на обеспечение благополучия граждан в цифровом пространстве (в том числе программ начальной школы) [10; 20]. Однако проблема информационной безопасности обучающихся по-прежнему стоит крайне остро.

Кроме того, особые информационные риски появляются в контексте возникшей в последние годы пандемии коронавирусной инфекции COVID-19. В профессиональном сообществе обсуждаются тенденции увеличения экранного времени как среди взрослых, так и среди детей по разным причинам (например, учеба, избыток свободного времени, поиск информации и т.д.). Безусловно, специалисты отмечают риск развития киберзависимости у детей различных возрастных групп, начиная с младших школьников [11; 19].

В докладе Объединенного исследовательского центра Службы науки и знаний Европейской комиссии (Joint Research Centre, European Commission) подчеркивается, что современные дети к тому времени, когда они закончат образование, будут использовать больше технологий, чем любой из поколения ныне работающих взрослых [7]. Таким обра-

зом, очевидно, что школьники должны быть надлежащим образом оснащены средствами защиты от различных киберугроз.

В этой связи проведение социологического исследования для выявления владения обучающимися знаниями и умениями, связанными с распознаванием информационных угроз, а также позволяющими противодействовать этим угрозам, представляется весьма актуальным и своевременным.

На данный момент существует ряд социологических исследований, связанных с оценкой воздействия информационной среды на личность человека, в частности, обучающегося. Так, в крупномасштабных исследованиях, проводившихся сотрудниками Центра социологии образования РАО (под руководством академика РАО В.С. Собкина), выполнен анализ значимости новых информационных технологий в структуре досуга и информационном пространстве современного ребенка [1—5]. В рамках этих исследований рассматривались содержательные особенности интереса учащихся к миру компьютеров, роль и место новых информационных технологий в образовательном процессе и влияние регулярного пользования компьютером на академическую успеваемость учащихся. Более того, исследователи Института управления образованием РАО ранее проводили социологические исследования в области доступности средств информатизации в образовательных организациях российских регионов [14; 18].

В данной статье приводятся результаты социологического исследования, направленного на выявление уровня киберугроз, которым подвергаются современные российские школьники (на материале опроса обучающихся 7—11 классов общеобразовательных школ регионов Российской Федерации).

## Методы

В рамках исполнения государственного задания Министерства просвещения Российской Федерации сотрудниками ФГБНУ «Институт управления образованием Российской академии образования» были разработаны программа и инструментарий социологического исследования (анкета для учащихся 7—11 классов общеобразовательных школ).

Инструментарий социологического исследования позволяет выявлять уровень владения обучающимися знаниями и умениями, связанными с распознаванием информационных угроз и позволяющими противодействовать этим угрозам. Структура анкетного опросника предполагает наличие специальных блоков вопросов, направленных на изучение различных аспектов, связанных с информационной безопасностью обучающихся в цифровой среде.

План выборки по согласованным с Министерством просвещения Российской Федерации регионам построен по кластерному принципу. При подготовке исследования реализован принцип кластеризации генеральной совокупности: в качестве кластеров выступили следующие 7 субъектов Российской Федерации: Калининградская область, Ленинградская область, Московская область, Приморский край, Республика Крым, Республика Саха (Якутия), Тамбовская область.

В социологическом исследовании был применен метод анкетного опроса, позволяющий выявить количественные и качественные оценки состояния киберрисков, которым подвергаются обучающиеся общеобразовательных школ, а также их готовность противостоять информационным угрозам. Опросник включает закрытые, открытые, поливариантные, альтернативные и ранговые вопросы, позволяющие охарактеризовать представления обучающихся об информационных угрозах, путях их преодоления. Полученные данные обработаны методами математической статистики с помощью статистического пакета программ SPSS и STATISTICA.

Социологический опрос проводился в ноябре 2020 года. Сбор данных был организован в регионах исследования на официальном сайте ФГБНУ «Институт управления образованием Российской академии образования» (www.iuorao.ru) с применением сервиса электронных опросов.

Всего в ходе проведения исследования было опрошено 5682 обучающихся 7—11 классов общеобразовательных школ из

разных регионов России. Исследуемую выборочную совокупность составили 2586 мальчиков (45,5%) и 3096 девочек (54,5%).

### Результаты

В ходе проведения исследования респондентам был предложен целый ряд вопросов, посвященных выявлению степени владения школьниками методами и средствами защиты информации и противодействия информационным угрозам личности.

Одним из факторов, определяющих кибербезопасность личности, является способность человека оценить полученную информацию на предмет ее истинности и актуальности. В ходе опроса школьники отмечали, каким образом они оценивают достоверность полученных сведений в сети Интернет. Распределение ответов приведено в табл. 1.

Таблица 1

**Распределение ответов респондентов на вопрос «Как Вы оцениваете достоверность полученных сведений?», в %**

| Вариант ответа | % |
|---|---|
| Сравниваю с другими сведениями на ту же тему | 63,3 |
| Думаю, что все само прояснится в будущем | 11,2 |
| Не пытаюсь оценить достоверность | 9,1 |
| Не верю никаким источникам | 7,9 |
| Верю источнику сведений | 7,3 |
| Другие способы | 1,4 |

Как видно из приведенных данных, большинство школьников применяют продуктивную стратегию проверки полученных сведений — сравнение с альтернативными источниками информации. Так ответили 63,3% опрошенных. Однако важно заметить, что пассивные стратегии, такие как «думаю, что все само прояснится в будущем», «не пытаюсь оценить достоверность», «верю источнику сведений», применяют более четверти опрошенных школьников. Таким образом, можно отметить, что в целом большинство опрошенных обучающихся склонны критически относиться к информации, полученной ими в Сети, и не принимать на веру полученные сведения. При этом пассивная стратегия четверти школьников — склонность доверять полученной в интернете информации без ее специальной проверки — вызывает некоторую тревогу в отношении рисков возникновения киберугроз.

Кроме того, респондентов просили указать, каким образом они предполагают защищаться от провокационной информации, высказанной в их адрес в сети Интернет (если такое произойдет). Полученные результаты показали, что большинство подростков предпочитают стратегию избегания — не будут обращать внимание на подобные провокации (59,5%) или прекратят общение (46,3%). Значительно меньшее число школьников указало, что в подобной ситуации обратятся за помощью: к взрослым (родителям, учителям) — 29,2%, к друзьям — 13,8%. Выявленная тенденция подтверждает результаты описанных выше исследований о высокой вероятности попыток школьников самостоятельно справиться с киберугрозами. Данный результат акцентирует внимание психолого-педагогического сообщества на необходимости владения школьниками средствами информационной защиты, чтобы подросток имел возможность самостоятельно справиться с подобными угрозами.

В ходе опроса респонденты также отмечали, являются ли, на их взгляд, ограничительные меры действенным средством защиты от недоброкачественной информации. Как показали результаты, мнения школьников распределились примерно в равных пропорциях: 38,3% считают, что являются, 29,9% ответили отрицательно, при этом 31,8% затруднились дать ответ на данный вопрос.

Значительное внимание в исследовании уделялось выявлению знаний и представлений школьников о различных понятиях, связанных с кибербезопасностью. В частности, оценивались знания школьников относительно современных технологий. Так, в ходе исследования был задан специальный вопрос «Какие технологии Вы бы отнесли к технологиям будущего?». Распределение ответов приведено в табл. 2.

Таблица 2

**Распределение ответов респондентов на вопрос «Какие технологии Вы бы отнесли к технологиям будущего?», в %**

| Вариант ответа | % |
|---|---|
| Дополненную реальность | 56,0 |
| Робототехнику | 50,6 |
| 3D—печать | 50,2 |
| Облачные технологии | 18,7 |
| Интернет вещей | 11,3 |
| Ничего из перечисленного | 10,3 |
| Не знаю | 10,2 |
| Другие | 2,3 |

Как видно из приведенных в таблице данных, большинство опрошенных относят к технологиям будущего дополненную реальность, робототехнику и 3D—печать. Другие ответы назывались значительно реже. При этом каждый десятый школьник (10,2%) затруднился дать ответ на данный вопрос.

Одним из важнейших вопросов данного исследования является выявление знаний и представлений школьников о таком понятии, как «кибератака». В ходе опроса школьникам предлагалось выбрать из представленных вариантов ответа, что, по их мнению, понимается под кибератакой. Ответы на данный вопрос представлены в табл. 3.

Таблица 3

**Распределение ответов респондентов на вопрос «Что Вы понимаете под кибератакой?», в %**

| Вариант ответа | % |
|---|---|
| Желание завладеть Вашими информационными ресурсами | 66,3 |
| Внедрение в Ваш компьютер вируса | 45,0 |
| Попытка испортить программное обеспечение Вашего компьютера | 32,0 |
| Воздействие на Вашу личность | 21,7 |
| Не знаю | 16,2 |
| Желание отключить Вас от интернета | 6,4 |
| Другое | 1,4 |

Как видно из таблицы, под кибератакой школьники наиболее часто понимают: желание завладеть информационными ресурсами, внедрение вируса, попытку испортить программное обеспечение компьютера. Лишь каждый пятый опрошенный (21,7%) указал на такой феномен, как воздействие на личность человека. Таким образом, можно сделать вывод, что современные школьники в целом владеют знаниями в области кибербезопасности и противодействия информационным угрозам. Однако очевидно, что такой фактор, как воздействие на личность, довольно редко учитывается ими в данном контексте.

И наконец, обсуждая вопросы кибербезопасности, важно обратиться к проблеме хранения и защиты данных. В ходе исследования обучающихся просили указать, как они предпочитают защищать важную для них информацию. Распределение ответов приведено в табл. 4.

Таблица 4

**Распределение ответов респондентов на вопрос «Как Вы предпочитаете защищать важную для Вас информацию?», в %**

| Вариант ответа | % |
|---|---|
| На компьютере, защищенном паролем | 40,1 |
| Скрыть, сделать ее незаметной | 34,7 |
| На личном носителе (диск, карта памяти и др.) | 31,3 |
| В архиве, открыть который можно только с помощью пароля | 30,8 |
| В облачном хранилище данных или в интернет-хранилище | 19,7 |
| Не применяю никаких особых средств | 12,4 |
| Другое | 4,2 |

Как видно из таблицы, большинство учащихся предпочитают защищать свою информацию на своем персональном компьютере при помощи пароля (40,1%) или в архивной папке (30,8%), треть опрошенных предпочитает каким-либо образом скрыть важную для них информацию (34,7%) или хранить ее на личном носителе (31,3%). Кроме того, важным способом защиты информации среди современных подростков является облачное хранилище данных (19,7%).

Использованию облачных хранилищ информации в исследовании было уделено отдельное внимание. Результаты опроса пока-

зали, что половина опрошенных школьников (50,8%) пользуются облачными сервисами хранения информации. При этом ответы респондентов свидетельствуют о сомнениях обучающихся относительно защищенности информации, хранящейся в облаке. Так, полностью безопасными облачные хранилища считает лишь каждый пятый опрошенный (19,6%), 48,9% оценивают их как «частично защищенные», 15,2% считают, что для достаточной степени защиты информации в облаке необходим пароль, а 16,3% указали, что не доверяют такому способу хранения информации.

В ходе исследования школьников также просили указать, как лучше всего защитить информацию на персональном компьютере. Распределение ответов респондентов на данный вопрос приведено в табл. 5.

Таблица 5

**Распределение ответов респондентов на вопрос «Как лучше всего защитить важную информацию на компьютере?», в %**

| Вариант ответа | % |
|---|---|
| Копировать на внешний носитель | 53,6 |
| Сохранить в облаке | 21,6 |
| Не знаю | 15,8 |
| Другим способом | 4,7 |
| Послать по почте себе или другу | 4,4 |

Приведенные в таблице данные показывают, что, по мнению обучающихся, наиболее эффективными способами защиты информации являются копирование на внешний носитель и сохранение в облачном хранилище. Однако важно отметить, что 15,8% затруднились ответить на данный вопрос.

Таким образом, полученные результаты позволяют отметить, что современные обучающиеся достаточно хорошо владеют знаниями о различных методах и средствах защиты информации и противодействия киберугрозам. Однако исследование позволило выявить некоторые дефициты в знаниях школьников и невозможность самостоятельно оценить серьезность всех киберрисков и угроз, с которыми они могут столкнуться при применении информационных технологий. Это представляется значительным вызовом для современной системы образования.

В этой связи следует обратиться к изучению роли системы образования в овладении современными детьми методами и средствами кибербезопасности. Подчеркнем, что отдельное внимание в исследовании уделялось образовательным аспектам — проводятся ли в школе специальные обучающие мероприятия по профилактике и противодействию киберугрозам. Обучающимся задавался вопрос «Рассказывают ли Вам в школе про информационную безопасность?», ответы на который характеризовали те предметные дисциплины, в рамках которых проводилась работа по данной проблематике. Ответы респондентов приведены в табл. 6.

Таблица 6

**Распределение ответов респондентов на вопрос «Рассказывают ли Вам в школе про информационную безопасность?», в %**

| Вариант ответа | % |
|---|---|
| Да, на уроках информатики | 63,3 |
| Да, на уроках ОБЖ | 38,5 |
| Да, на уроках обществоведения | 21,4 |
| Нет | 18,1 |
| Да, на уроках технологии | 8,5 |
| Да, на других уроках | 6,2 |

Как видно из таблицы, школьники довольно часто указывают на наличие подобных занятий. При этом наиболее часто называют уроки информатики, ОБЖ и обществоведения.

Также в ходе опроса выявлялась регулярность проведения в школе мероприятий (открытых уроков, классных часов и др.) по видам информации в сети Интернет, которая может причинить вред их здоровью и развитию. Результаты исследования показали, что подобные занятия проводятся в образовательных организациях достаточно регулярно: 45,0% опрошенных указали, что они проводились два и более раз, 28,3% — проводились один раз. Однако заметим, что 26,8% школьников ответили, что в их школе не проводилось подобных профилактических мероприятий.

Кроме того, опрошенных учеников просили оценить, помогут ли знания, полученные

в школе, найти защиту от информационных угроз. Исследование показало, что большинство школьников положительно оценивают знания, полученные в школе, в области кибербезопасности: 18,5% ответили, что полученные знания им «безусловно помогут», 42,1% — «скорее помогут». Однако более трети опрошенных отмечают недостаточность этих знаний: 25,9% — «скорее не помогут», 13,5% — «точно не помогут».

Таким образом, можно сделать вывод о том, что в современных образовательных организациях уделяется внимание профилактике различных информационных угроз на уроках информатики, ОБЖ и обществоведения, а также проводятся специальные мероприятия по видам информации в сети Интернет, которая может причинить вред здоровью и развитию ребенка. Однако очевидно, что в связи с актуальностью данной проблематики требуется проведение более системной и регулярной работы с обучающимися.

## Обсуждение

Проведенное социологическое исследование, посвященное выявлению степени владения школьниками методами и средствами защиты информации и противодействия информационным угрозам личности, позволило сделать ряд содержательных выводов.

Во-первых, следует отметить, что современные школьники в целом владеют знаниями о различных методах и средствах защиты информации и противодействия киберугрозам. При этом выявлены некоторые дефициты в знаниях и представлениях обучающихся о факторах риска при пользовании информационными сетями. В частности, такой фактор, как воздействие на личность, довольно редко учитывается школьниками в данном контексте.

В этой связи важно обратить внимание психолого-педагогической общественности на выявленные дефициты в знаниях школьников и их трудности при самостоятельной оценке киберрисков и угроз, с которыми они могут столкнуться при применении информационных технологий. В частности, несмотря на то, что в целом большинство обучающихся склонны критически относиться к информации, полученной ими в Сети, и не принимать на веру полученные сведения, пассивная стратегия четверти школьников — склонность доверять полученной в интернете информации без ее специальной проверки — вызывает некоторую тревогу в отношении рисков возникновения киберугроз. Безусловно, все перечисленное представляется значительным вызовом для современной системы образования.

Второй важный вывод связан с тем, что в современных образовательных организациях в целом уделяется внимание профилактике различных информационных угроз на уроках информатики, ОБЖ и обществоведения, а также проводятся специальные мероприятия по видам информации в сети Интернет, которая может причинить вред здоровью и развитию ребенка. Однако очевидно, что в связи с актуальностью данной проблематики требуется проведение более системной и регулярной работы с обучающимися.

## Заключение

Представленные материалы показывают актуальность и значимость комплексного и междисциплинарного изучения вопросов, связанных с киберрисками, с которыми сталкиваются современные подростки, в контексте совершенствования образовательных подходов и программ в данной области. Развитие социальных сетей и возрастание их влияния на все сферы жизни детей и молодежи является значительным вызовом современного общества. В этой связи необходимы системные управленческие решения как по предотвращению киберугроз и негативного влияния компьютерных сетей на ребенка, так и по развитию регулярной системной работы с обучающимися в образовательных организациях, что в первую очередь связано с необходимостью обеспечения психологического благополучия обучаемых.

Выявленные «проблемные точки» в обсуждаемой теме требуют дальнейшего изучения, обсуждения их содержания в научной среде, а также последующего проектирования эффективных механизмов управления образовательными системами в ситуациях, связанных с киберрисками и киберкризисами.

***Литература***

1. *Собкин В.С., Адамчук Д.В.* Мониторинг социальных последствий информатизации: что изменилось в школе за три года? М.: Институт социологии образования РАО, 2008. 159 с.
2. *Собкин В.С., Евстигнеева Ю.М.* Подросток: виртуальная и социальная реальность // Труды по социологии образования. Т. VI. Вып. X. / Под ред. В.С. Собкина. М.: Центр социологии образования РАО, 2001. 156 с.
3. *Собкин В.С., Скобельцина К.Н.* Представления родителей об особенностях общения их ребенка с компьютером // Современное дошкольное образование. 2012. № 3. С. 30—34.
4. *Собкин В.С., Федотова А.В.* Подростковая агрессия в социальных сетях: восприятие и личный опыт // Психологическая наука и образование. 2019. Том 24. № 2. С. 5—18. DOI:10.17759/pse.2019240201
5. *Собкин В.С., Федотова А.В.* Сеть как пространство социализации современного подростка // Консультативная психология и психотерапия. 2019. Том 27. № 3. С. 119—137. DOI:10.17759/cpp.2019270308
6. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_108808/ (дата обращения: 09.07.2021).
7. *Brittan T., Jahankhani H., McCarthy J.* An Examination into the Effect of Early Education on Cyber Security Awareness Within the U.K. / In Jahankhani H. (ed.) // Cyber Criminology. Advanced Sciences and Technologies for Security Applications. Springer, Cham, 2018. DOI:10.1007/978-3-319-97181-0_14
8. Cyberbulling as A New Form of a Threat: A Physiological, Psychological and Medicinal Aspects / Mikhaylovsky M.N., Lopatkova I.V., Komarova N.M., Rueva E.O., Tereschuk K.S., Emelyanenkova A.V. [Электронный ресурс] // Electronic Journal of General Medicine. 2019. Vol. 16. № 6. DOI:10.29333/ejgm/114268
9. Cyberbullying Among Greek High School Adolescents / Gkiomisi A., Gkrizioti M., Gkiomisi A., Anastasilakis D., Kardaras P. // Indian J Pediatr. 2017. Vol. 84. № 5. P. 364—368. DOI:10.1007/s12098-016-2256-2
10. Cybersecurity Baseline, An Exploration, Which Permits to Delineate National Cybersecurity Strategy in Ecuador / Ron M., Rivera O., Fuertes W., Toulkeridis T., Díaz J. // In Rocha Á., Ferrás C., Paredes M. (eds.) Information Technology and Systems. Springer, Cham, 2019. DOI:10.1007/978-3-030-11890-7_79
11. *Dishkova M., Papancheva R.* Estimation of Parents' Opinion How the Time Spent in Front of a Screen for Learning Affects the Likelihood of Developing Cyber-Addiction in Children in Primary School // ICERI 2020 Proceedings (Online Conference, 9—10 November 2020). IATED Academy. 2020. P. 8925—8933. DOI:10.21125/iceri.2020
12. Is Cyberbullying Related to Trait or State Anger? / Lonigro A., Schneider B., Laghi F., Baiocco R., Pallini S., Brunner T. // Child Psychiatry and Human Development. 2015. Vol. 46. № 3. P. 445—454. DOI:10.1007/s10578-014-0484-0
13. *Kniffin K.M., Palacio D.* Trash-Talking and Trolling // Human Nature. 2018. № 29. P. 353—369. DOI:10.1007/s12110-018-9317-3
14. *Kuznetsov A., Skobeltsina K.* Social Educational Infrastructure for Russian School Students: Baseline Study in Availability and Accessibility under Regular and Critical Conditions // INTED2021 Proceedings (Online Conference, 8-9 March 2021). IATED Academy. 2021. P. 8247—8251. DOI:10.21125/inted.2021.1676
15. *Legate N., Weinstein N., Przybylski A.K.* Parenting Strategies and Adolescents' Cyberbullying Behaviors: Evidence from a Preregistered Study of Parent—Child Dyads // J Youth Adolescence. 2019. Vol. 48. № 2. P. 399—409. DOI:10.1007/s10964-018-0962-y
16. *Nicolaidou I., Venizelou A.* «Be Smart When Online!»: Kids Learn How to Protect Personal Data, Stop Cyber-Bullying and Avoid Hackers // ICERI2016 Proceedings (Seville, Spain, 14—16 November 2016). IATED Academy. 2016. P. 3374—3384. DOI:10.21125/iceri.2016.1789
17. *Shutikova M., Beshenkov S.* Digital Educational Environment and Media Education — Platforms for Transforming Education System // Медиаобразование. 2020. Том 60. № 4. С. 736—744. DOI:I0.i3i87/me.2020.4.736
18. *Skobeltsina K.N., Kuznetsov A.N.* Research on Public Satisfaction with Educational Infrastructure of Advanced Development Territories // Proceedings of the 9th International Conference for Science Educators and Teachers (Moscow, Russia, 4-5 April 2019). Atlantis Press. 2019. P. 36—41. DOI:10.2991/icdee-19.2019.7
19. SMERF: Social Media, Ethics and Risk Framework / Mitchell I., Cockerton T., Hara S., Evans C. // In Jahankhani H. (ed.) Cyber Criminology. Advanced Sciences and Technologies for Security Applications. Springer, Cham, 2018. DOI:10.1007/978-3-319-97181-0_10
20. Toward Digital Citizenship in Primary Schools: Leveraging on Our Enhanced Cyberwellness Framework / Lim W.Y., Tan C.M., Nizam M., Zhou W., Tan S.M. // In Chai C., Lim C., Tan C. (eds.) Future Learning in Primary Schools. Springer, Singapore. 2016. DOI:10.1007/978-981-287-579-2_7
21. Utilizing Temporal Psycholinguistic Cues for Suicidal Intent Estimation / Mathur P., Sawhney R., Chopra S., Leekha M., Ratn Shah R. // In Jose J. et al. (eds.) Advances in Information Retrieval. Springer, Cham, 2020. DOI:10.1007/978-3-030-45442-5_33
22. *Yildiz Durak H.* Cyber Human Values Displayed by University Students in Online Social Networking Sites: The Relationship of Cyber Human Values to

Cyberbullying and Cyber Victimization Behaviors // INTED2019 Proceedings (Valencia, Spain, 11—13 March 2019). IATED Academy. 2019. P. 10035—10038. DOI:10.21125/inted.2019.2531

***References***

1. Sobkin V.S., Adamchuk D.V. Monitoring sotsial'nykh posledstvii informatizatsii: chto izmenilos' v shkole za tri goda? [Monitoring the social consequences of informatization: what has changed at school in three years?]. Moscow: Publ. Institut sotsiologii obrazovaniya RAO, 2008. 159 p. (In Russ.).
2. Sobkin V.S., Evstigneeva Yu.M. Podrostok: virtual'naya i sotsial'naya real'nost' [Teenager: virtual and social reality]. In Sobkin V.S. (ed.), *Trudy po sotsiologii obrazovaniya*. T. 6. Vyp. 10. [*Works on the sociology of education*. Vol. 6. No. 10.]. Moscow: Publ. Center sotsiologii obrazovaniya RAO, 2001. 156 p. (In Russ.).
3. Sobkin V.S., Skobel'tsina K.N. Predstavleniya roditelei ob osobennostyakh obshcheniya ikh rebenka s komp'yuterom [Parents' ideas about the peculiarities of their child's communication with a computer]. *Sovremennoe doshkol'noe obrazovanie = Modern preschool education*, 2012, no. 3, pp. 30—34. (In Russ.).
4. Sobkin V.S., Fedotova A.V. Podrostkovaya agressiya v sotsial'nykh setyakh: vospriyatie i lichnyi opyt [Teenage aggression in social networks: perception and personal experience]. *Psikhologicheskaya nauka i obrazovanie = Psychological Science and Education*, 2019. Vol. 24, no. 2, pp. 5—18. DOI:10.17759/pse.2019240201 (In Russ.).
5. Sobkin V.S., Fedotova A.V. Set' kak prostranstvo sotsializatsii sovremennogo podrostka [Network as a space of socialization of a modern teenager]. *Konsul'tativnaya psikhologiya i psikhoterapiya = Counseling Psychology and Psychotherapy*, 2019. Vol. 27, no. 3, pp. 119—137. DOI:10.17759/cpp.2019270308 (In Russ.).
6. Federal'nyi zakon ot 29.12.2010 № 436-FZ «O zashchite detei ot informatsii, prichinyayushchei vred ikh zdorov'yu i razvitiyu» [Federal Law of December 29, 2010 No. 436-FZ «On the Protection of Children from Information Harmful to Their Health and Development»]. Spravochnaya pravovaya sistema «Konsul'tantPlyus» [Reference legal system «ConsultantPlus»]. Available at: http://www.consultant.ru/document/cons_doc_LAW_108808/ (Accessed 09.07.2021). (In Russ.).
7. Brittan T., Jahankhani H., McCarthy J. An Examination into the Effect of Early Education on Cyber Security Awareness Within the U.K. In Jahankhani H. (ed.), *Cyber Criminology. Advanced Sciences and Technologies for Security Applications*. Springer, Cham, 2018. DOI:10.1007/978-3-319-97181-0_14
8. Mikhaylovsky M.N. et al. Cyberbulling as A New Form of a Threat: A Physiological, Psychological and Medicinal Aspects. *Electronic Journal of General Medicine*, 2019. Vol. 16, no. 6. DOI:10.29333/ejgm/114268
9. Gkiomisi A. et al. Cyberbullying Among Greek High School Adolescents. *Indian J Pediatr*, 2017. Vol. 84, no. 5, pp. 364—368. DOI:10.1007/s12098-016-2256-2
10. Ron M. et al. Cybersecurity Baseline, An Exploration, Which Permits to Delineate National Cybersecurity Strategy in Ecuador. In Rocha Á., Ferrás C., Paredes M. (eds.) *Information Technology and Systems*. Springer, Cham, 2019. DOI:10.1007/978-3-030-11890-7_79
11. Dishkova M., Papancheva R. Estimation of Parents' Opinion How the Time Spent in Front of a Screen for Learning Affects the Likelihood of Developing Cyber-Addiction in Children in Primary School. *ICERI 2020 Proceedings* (Online Conference, 9—10 November 2020). IATED Academy, 2020, pp. 8925—8933. DOI:10.21125/iceri.2020
12. Lonigro A. et al. Is Cyberbullying Related to Trait or State Anger? *Child Psychiatry and Human Development*, 2015. Vol. 46, no. 3, pp. 445—454. DOI:10.1007/s10578-014-0484-0
13. Kniffin K.M., Palacio D. Trash-Talking and Trolling. *Human Nature*, 2018, no. 29, pp. 353—369. DOI:10.1007/s12110-018-9317-3
14. Kuznetsov A., Skobeltsina K. Social Educational Infrastructure for Russian School Students: Baseline Study in Availability and Accessibility under Regular and Critical Conditions. *INTED2021 Proceedings* (Online Conference, 8—9 March 2021). IATED Academy, 2021, pp. 8247—8251. DOI:10.21125/inted.2021.1676
15. Legate N. et al. Parenting Strategies and Adolescents' Cyberbullying Behaviors: Evidence from a Preregistered Study of Parent—Child Dyads. *J Youth Adolescence*, 2019. Vol. 48, no. 2, pp. 399—409. DOI:10.1007/s10964-018-0962-y
16. Nicolaidou I., Venizelou A. «Be Smart When Online!»: Kids Learn How to Protect Personal Data, Stop Cyber-Bullying and Avoid Hackers. *ICERI2016 Proceedings* (Seville, Spain, 14—16 November 2016). IATED Academy, 2016, pp. 3374—3384. DOI:10.21125/iceri.2016.1789
17. Shutikova M., Beshenkov S. Digital Educational Environment and Media Education — Platforms for Transforming Education System. *Mediaobrazovanie = Media Education*, 2020. Vol. 60, no. 4, pp. 736—744. DOI:l0.i3i87/me.2020.4.736
18. Skobeltsina K.N., Kuznetsov A.N. Research on Public Satisfaction with Educational Infrastructure of Advanced Development Territories. *Proceedings of the 9th International Conference for Science Educators and Teachers* (Moscow, Russia, 4—5 April 2019). Atlantis Press, 2019, pp. 36—41. DOI:10.2991/icdee-19.2019.7
19. Mitchell I. et al. SMERF: Social Media, Ethics and Risk Framework. In Jahankhani H. (ed.) *Cyber Criminology. Advanced Sciences and Technologies*

*for Security Applications*. Springer, Cham, 2018. DOI:10.1007/978-3-319-97181-0_10
20. Lim W.Y. et al. Toward Digital Citizenship in Primary Schools: Leveraging on Our Enhanced Cyberwellness Framework. In Chai C., Lim C., Tan C. (eds.) *Future Learning in Primary Schools*. Springer, Singapore, 2016. DOI:10.1007/978-981-287-579-2_7
21. Mathur P. et al. Utilizing Temporal Psycholinguistic Cues for Suicidal Intent Estimation. In Jose J. et al. (eds.) *Advances in Information Retrieval*. Springer, Cham, 2020. DOI:10.1007/978-3-030-45442-5_33
22. Yildiz Durak H. Cyber Human Values Displayed by University Students in Online Social Networking Sites: The Relationship of Cyber Human Values to Cyberbullying and Cyber Victimization Behaviors. *INTED2019 Proceedings* (Valencia, Spain, 11—13 March 2019). IATED Academy, 2019, pp. 10035—10038. DOI:10.21125/inted.2019.2531

***Информация об авторах***
*Скобельцина Ксения Николаевна*, кандидат психологических наук, ученый секретарь, ведущий научный сотрудник Центра управления образовательными системами, ФГБНУ «Институт управления образованием Российской академии образования» (ФГБНУ ИУО РАО), г. Москва, Российская Федерация, ORCID: https://orcid.org/0000-0003-0673-7620, e-mail: skobeltsina@iuorao.ru

*Кузнецов Андрей Николаевич*, кандидат педагогических наук, доцент, заместитель директора по научной работе, руководитель Центра управления образовательными системами, ФГБНУ «Институт управления образованием Российской академии образования» (ФГБНУ ИУО РАО), г. Москва, Российская Федерация, ORCID: https://orcid.org/0000-0003-1573-5491, e-mail: kuznetsov@iuorao.ru

*Бешенков Сергей Александрович*, доктор педагогических наук, профессор, главный научный сотрудник Центра содержания и методов обучения, ФГБНУ «Институт управления образованием Российской академии образования» (ФГБНУ ИУО РАО), г. Москва, Российская Федерация, ORCID: https://orcid.org/0000-0001-7225-5924, e-mail: srg57@mail.ru

***Information about the authors***
*Ksenia N. Skobeltsina*, PhD in Psychology, Academic Secretary, Leading Researcher, Center for Educational Systems Management, Institute of Education Management of the Russian Academy of Education, Moscow, Russia, ORCID: https://orcid.org/0000-0003-0673-7620, e-mail: skobeltsina@iuorao.ru

*Andrei N. Kuznetsov*, PhD in Pedagogy, Associate Professor, Deputy Director for Research, Head of Center for Educational Systems Management, Institute of Education Management of the Russian Academy of Education, Moscow, Russia, ORCID: https://orcid.org/0000-0003-1573-5491, e-mail: kuznetsov@iuorao.ru

*Sergey A. Beshenkov*, Doctor of Pedagogy, Professor, Chief Researcher, Center for Content and Teaching Methods, Institute of Education Management of the Russian Academy of Education, Moscow, Russia, ORCID: https://orcid.org/0000-0001-7225-5924, e-mail: srg57@mail.ru

Получена 13.07.2021
Принята в печать 11.08.2021

Received 13.07.2021
Accepted 11.08.2021