https://edumag.mrsu.ru ISSN 1991-9468 (Print), 2308-1058 (Online)

СОЦИОЛОГИЯ ОБРАЗОВАНИЯ
SOCIOLOGY OF EDUCATION

https://doi.org/10.15507/1991-9468.029.202501.114-131
EDN: https://elibrary.ru/mcpwtu
УДК / UDC 004.9-027.45:303-053.6
Оригинальная статья / Original article

Цифровая безопасность подростков: социологический анализ

С. Г. Ушкин [1, 2, 3], ***Е. А. Коваль*** [3, 4], ***М. Д. Мартынова*** [3] ✉
[1] *Научный центр социально-экономического мониторинга, г. Саранск, Российская Федерация*
[2] *Всероссийский центр изучения общественного мнения, г. Москва, Российская Федерация*
[3] *МГУ им. Н. П. Огарёва, г. Саранск, Российская Федерация*
[4] *Средне-Волжский институт (филиал) ВГУЮ (РПА Минюст России), г. Саранск, Российская Федерация*
✉ *martynovamd@mail.ru*

Аннотация

Введение. Рост объемов персональных данных, размещаемых пользователями на платформах социальных сетей, интенсификация сбора пользовательского контента для машинного обучения представляет собой значимый вызов информационного общества. Влияние новых цифровых инструментов на стратегии обеспечения пользователями своей безопасности в сети Интернет требует тщательного изучения. В фокусе работы – подростки, которые представляют одну из рискогенных групп. Цель исследования – определение представлений подростков об опасениях, связанных с их персональными данными, а также их сравнение в двух разных российских регионах.

Материалы и методы. Эмпирическая база представлена данными социологического исследования, проведенного в 2023–2024 гг. методом онлайн-опроса среди учащихся 8–11 классов в двух российских регионах – Республике Мордовия и Донецкой Народной Республике. Выборка квотная, репрезентирует каждый из регионов по отдельности.

Результаты исследования. Полученные результаты демонстрируют беспокойство половины опрошенных относительно сбора персональных данных. Преобладающая часть респондентов негативно относится к попаданию данных и размещаемого контента в большие массивы и использованию для машинного обучения. Российские подростки амбивалентно относятся к конфиденциальности в цифровом пространстве. Фиксируется «парадокс конфиденциальности», когда пользователи, осознавая негативные последствия, продолжают размещать информацию о себе с целью сиюминутной выгоды. Сбор данных для обучения нейросетей воспринимается отрицательно. Забота о цифровой безопасности не является распространенной практикой, что релевантно для подростков обоих регионов, хотя школьники из Донецкой Народной Республики испытывают по этому поводу повышенную тревожность.

Обсуждение и заключение. Материалы статьи могут быть использованы для разработки образовательных программ и практических рекомендаций, направленных на повышение цифровой грамотности и формирование осознанных практик защиты персональных данных среди подростков, что является ключевым в условиях ведения гибридных войн и распространения мошеннических действий в виртуальном пространстве.

Ключевые слова: цифровая безопасность школьников, цифровые риски, защита персональных данных, большие данные, парадокс конфиденциальности, иллюзия приватности, большие языковые модели

Финансирование: исследование выполнено за счет гранта Российского научного фонда № 23-28-01288 (https://rscf.ru/project/23-28-01288/).

Благодарности: авторы выражают благодарность рецензентам за аргументированные замечания и рекомендации по доработке статьи; студентам МГУ им. Н. П. Огарёва Асташовой Е., Вдовиной А., Кастолиной А., Квашенковой Е., Лысенковой В., Самосудову Е. за организацию полевого этапа исследования в Республике Мордовия, студенту Донецкого государственного университета Занину Е. – в Донецкой Народной Республике.

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Для цитирования: Ушкин С.Г., Коваль Е.А., Мартынова М.Д. Цифровая безопасность подростков: социологический анализ. *Интеграция образования*. 2025;29(1):114–131. https://doi.org/10.15507/1991-9468.029.202501.114-131

Teenagers' Digital Security: Sociological Analysis

S. G. Ushkin [a, b, c], ***E. A. Koval*** [c, d], ***M. D. Martynova*** [c] ✉

[a] *Scientific Center for Socio-Economic Monitoring, Saransk, Russian Federation*

[b] *Russian Public Opinion Research Center, Moscow, Russian Federation*

[c] *National Research Mordovia State University, Saransk, Russian Federation*

[d] *Middle Volga Branch, All-Russian State University of Justice, Saransk, Russian Federation*

✉ *martynovamd@mail.ru*

Abstract

Introduction. The growing amount of personal data posted by users about themselves and other people on social media platforms, the intensification of user-generated content collection for machine learning determines the relevance of the research. The impact of new digital tools on users' online safety strategies needs to be scrutinized. The focus of the work is on adolescents, who represent one of the most risky groups. The aim of the study is to determine teenagers' perceptions of concerns related to their personal data and to compare them in two different Russian regions.

Materials and Methods. The empirical base is represented by the data of a sociological study conducted in 2023–2024 by online survey among schoolchildren of grades 8–11 in two Russian regions – the Republic of Mordovia and the Donetsk People's Republic. The sample is quota-based, representing each of the regions separately.

Results. Nearly half of respondents have some concerns about the collection of personal data. Most of them have negative attitudes towards their data and content being exposed to large datasets and used for machine learning. Teenagers fear that their data will be used for criminal purposes as well as financial loss. They believe that the surest way to ensure digital security is not to share their personal data unless it is necessary.

Discussion and Conclusion. The materials of the article can be used to develop educational programs and practical recommendations aimed at improving digital literacy and formation of conscious practices of personal data protection among teenagers. This is especially important in the current conditions of hybrid warfare and the spread of fraudulent activities in virtual space.

Keywords: school students' digital safety, digital risks, personal data protection, big data, privacy paradox, privacy illusion, large language models

Funding: The article was prepared with the financial support of the Russian Science Foundation, project No. 2328-01288 (https://rscf.ru/project/23-28-01288/).

Acknowledgements: The authors express their gratitude to the reviewers for their reasoned comments and recommendations for review of the article; to the students of National Research Mordovia State University Astashova E., Vdovina A., Kastolina A., Kvashenkova E., Lysenkova V., Samosudov E. for organizing the field stage of the research in the Republic of Mordovia, to the student of Donetsk State University Zanin E. – in the Donetsk People's Republic.

Conflict of interest: The authors declare no conflict of interest.

For citation: Ushkin S.G., Koval E.A., Martynova M.D. Teenagers' Digital Security: Sociological Analysis. *Integration of Education*. 2025;29(1):114–131. https://doi.org/10.15507/1991-9468.029.202501.114-131

Введение

Проблема обеспечения цифровой безопасности приобретает значение в условиях ускорения процессов цифровизации, вовлечения широких слоев населения в пользование цифровыми продуктами и сервисами. Интернет и социальные сети предоставляют пользователям беспрецедентные возможности по созданию и обмену данными, взаимодействию с ними и их смешению, агрегированию и систематизации. По данным ВЦИОМ, более 70 % детей и подростков применяют эти инструменты. Востребованными являются *WhatsApp* (42 %), *Telegram* (34 %) и «ВКонтакте» (27 %)[1]. Каждый человек становится производителем цифрового контента, который впоследствии может быть включен в наборы больших данных, используемых для анализа мнений людей и обучения передовых нейросетевых моделей.

Размещая личную информацию, пользователи предоставляют третьим лицам доступ к своим персональным данным, которые в дальнейшем могут быть скомпрометированы, создают угрозу утраты доверия и контроля над собственными репрезентациями. Иллюстрацией этого тезиса является рекламная кампания *Deutsche Telekom*: демонстрируются негативные последствия цифрового следа ребенка (начиная от интернет-травли, заканчивая кражей личных данных и созданием материалов сексуального насилия над детьми)[2]. Ее основной посыл заключается в том, что если в повседневной жизни сетевой контент представляет собой часть воспоминаний, то в технологическом измерении – это просто данные.

В связи с ростом цифровизации задачей государственного управления становится развитие инструментов обеспечения цифровой безопасности граждан посредством выстраивания грамотной образовательной политики, ключевыми реципиентами которой являются современные подростки – они более погружены в структуры виртуального взаимодействия, находя в них инструменты самовыражения, общения, поиска друзей и др. [1]. В зависимости от политики страны выделяются три группы решений по поддержанию цифрового суверенитета подростков: социальное (ответственность ложится на подростков и их окружение, в первую очередь родителей), юридическое (ответственность каждой из сторон нормативно детализируется), технологическое (дополнительные механизмы защиты внедряются технологическими компаниями) [2].

Исследования все чаще отмечают, что обеспечение цифровой безопасности подростков – обязанность родителей [3], однако информирование о растущей проблеме сохранения конфиденциальности требует образовательных усилий с участием школ, социальных сетей [4; 5] и правительственных учреждений, в первую очередь, законодательных органов [6]. Признавая значимость политических и правовых инструментов, ряд технологических компаний внедряют подход «конфиденциальность данных по замыслу»: персональная информация представляет собой фундаментальную ценность, которую необходимо защищать на всех этапах эксплуатации продукта или услуги[3] [7; 8]. Случай *Cambridge Analytica* способствовал дискредитации в массовых представлениях населения подобного рода практик. Получив доступ к данным пользователей *Facebook*[4], компания делала на основе их обработки таргетированную политическую рекламу, повлияв на результаты выборов в США и других странах [9].

Распоряжением Правительства РФ от 28 апреля 2023 г. № 1105-р утверждена Концепция информационной

[1] Детский кибербуллинг и как с ним бороться [Электронный ресурс] // ВЦИОМ : офиц. сайт. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/detskii-kiberbulling-i-kak-s-nim-borotsja (дата обращения: 03.09.2024).

[2] Telekom – Without Consent. A Message from Ella – Deutsche Telekom [Электронный ресурс]. URL: https://berlincommercial.awardsengine.com/?action=ows:entries.details&e=158295&project_year=2024 (дата обращения: 03.09.2024).

[3] de Chaves S. A., Barreto F., Benitti V. Privacy by Design in Software Engineering: An update of a Systematic Mapping Study // Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing. New York : Association for Computing Machinery, 2023. p. 1362–1369. https://doi.org/10.1145/3555776.3577626

[4] Facebook принадлежит компании Meta, признанной экстремистской организацией и запрещенной на территории Российской Федерации.

безопасности детей в Российской Федерации, приоритетом которой является совмещение трех обозначенных выше подходов, особая роль отводится деятельности государства и государственных институтов[5]. Подчеркивается, что «именно дети и подростки находятся в группе потенциального риска для негативного воздействия и интернет-манипуляций с последующим вовлечением в деструктивную деятельность», а информационная безопасность трактуется как «состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию»[6]. Этот тезис подтверждается замерами опросов ВЦИОМ среди граждан от 18 лет и старше: 58 % опрошенных убеждены в опасности современного мира для детей, 57 % – считают погруженность в гаджеты и компьютеры одним из главных рисков[7]. Подростки передают свои персональные данные не только близким, но и незнакомым людям по запросу в социальных сетях, при этом «…практически ни к кому не обращаются за помощью по вопросам, связанным с настройками приватности в Сети» [10].

Решение указанной проблемы – минимизация случаев попадания персональных данных подростков третьим лицам, однако появление нейросетей на основе больших данных, которые применяются для принятия социально значимых решений, делает такой выход бесперспективным. Интересы подростков перестанут быть видимыми для машинного зрения в случае исключения их данных из больших датасетов и принятия решений (политических, управленческих и др.) для социальных групп на основе аналитики [11–13]. Итогом станет проигрыш в борьбе за признание и ресурсы, поскольку конфиденциальная информация «…может иметь последствия для трудоустройства, страхового статуса и права на получение помощи или перспективы получить справедливое и непредвзятое отношение в судах и судебных процессах» [14]. Складывается следующая дилемма: с одной стороны, следует минимизировать размещение данных и контента в целях обеспечения своей цифровой безопасности, с другой – в условиях развития тесно связанных технологий больших данных и искусственного интеллекта необходимо обеспечить первоочередное поступление данных от лиц, в интересах которых будут приниматься решения на основе аналитики данных.

Наблюдается классическая «проблема вагонетки». Для того чтобы подростки могли выйти из этой развилки с минимальным для себя ущербом, необходимо обеспечить максимальный доступ к информации о возможных последствиях размещения персональных данных и передачи их третьим лицам, способах обеспечения цифровой безопасности в новых условиях – начиная от личной цифровой гигиены, заканчивая обеспечением государственного контроля в этой сфере.

Насколько дети и подростки обеспокоены по поводу своей цифровой безопасности и безопасности своих данных? Каких последствий больше всего опасаются? На что они готовы пойти, чтобы их данные не попали третьим лицам, а контент не использовался без разрешения для машинного обучения? На эти и другие вопросы мы попытаемся ответить в данной статье.

Цель исследования – выявить опасения подростков относительно их персональных данных, определить различия в восприятии и практиках защиты своих данных у респондентов из «старого» и «нового» российских регионов.

Реализуя указанную цель, поставлены следующие задачи:

– выявить уровень беспокойства относительно конфиденциальности размещаемых подростками данных;

[5] Об утверждении Концепции информационной безопасности детей в Российской Федерации и признании утратившим силу Распоряжения Правительства РФ от 02.12.2015 г. № 2471-р : Распоряжение Правительства РФ от 28.04.2023 г. № 1105-р [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_446568/f62ee45faefd8e2a11d6d88941ac66824f848bc2/ (дата обращения: 03.09.2024).

[6] Там же.

[7] От чего нужно защищать современных детей? [Электронный ресурс] // ВЦИОМ : офиц. сайт. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/ot-chego-nuzhno-zashchishchat-sovremennykh-detei (дата обращения: 03.09.2024).

– определить отношение к сбору персональных данных пользователей машинными алгоритмами[8];

– проанализировать угрозы использования пользовательских данных;

– установить меры, применяемые подростками для защиты информации о себе.

Выдвинуты две гипотезы:

1. Подростки практически не испытывают чувства тревожности в отношении своих пользовательских данных, беспечны при их размещении и потенциальном использовании для машинного обучения.

2. Существуют различия в уровне тревожности относительно пользовательских данных, обусловленные территориальными признаками: в силу близости к местам ведения боевых действий подростки из «нового» российского региона более бдительно относятся к своей цифровой безопасности.

Обзор литературы

Понятие «цифровая безопасность» используется в общественном дискурсе, однако в российском законодательстве для обозначения безопасности детей применяется термин «информационная безопасность»[9]. Содержательно эти понятия различаются, несмотря на применение в одном семантическом поле. Понятие «кибербезопасность» синонимично цифровой безопасности [15].

В данном исследовании под цифровой безопасностью понимается состояние защищенности пользователя, пользовательских данных и контента в цифровой среде, включающей цифровые медиа, социальные сети, мессенджеры, платежные сети, информационно-образовательные платформы и др. Оперируя этим понятием, следует учитывать, что «цифровая безопасность предполагает не только “защиту цифры”, но и “защиту от цифры”» [16].

Ученые, анализирующие проблемы информационной безопасности подростков, акцентируют внимание на трех ключевых вопросах: обеспечении цифровой грамотности подростков через образовательные технологии [17], правовые механизмы цифровой безопасности [18; 19], консолидации усилий всех сторон цифровой безопасности, включая производителей цифровых продуктов [20]. Разработка способов обеспечения цифровой безопасности подростков осуществляется с опорой на результаты исследований их цифровой компетентности, учитывается разница между эмоциональными реакциями и уровнем компетентности подростков[10].

Ключевым компонентом цифровой безопасности является конфиденциальность – требование субъекту, получившему доступ к информации, не передавать ее кому-либо без согласия обладателя[11]. Несмотря на наличие регулирующего порядок обеспечения конфиденциальности и цифровой безопасности законодательства, локальных актов компаний с подробными соглашениями о конфиденциальности, большое количество методических материалов и обучающих мероприятий, конфиденциальность пользователей постоянно нарушается. Для обеспечения цифровой безопасности подросткам недостаточно владеть навыками установки безопасного пароля, двухфакторной аутентификации,

[8] Данная задача особенно актуальна, поскольку появились большие языковые модели, для обучения которых требуются большие наборы данных (включая контент, размещаемый в социальных сетях). Наиболее результативные продукты, в частности модели компании OpenAI, стали широкодоступными в конце 2022 г. Подростки, погруженные в цифровое пространство, осведомлены о сборе данных для больших языковых моделей машинными алгоритмами, и это могло повлиять на их отношение к размещению своих данных в интернете.

[9] О защите детей от информации, причиняющей вред их здоровью и развитию : федер. закон от 29.12.2010 г. № 436-ФЗ [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_108808/b819c620a8c698de35861ad4c9d9696ee0c3ee7a/ (дата обращения: 03.09.2024).

[10] Солдатова Г. У., Рассказова Е. И., Нестик Т. А. Цифровое поколение России: компетентность и безопасность. М. : Смысл, 2017. 375 с. URL: https://bmu.vrn.muzkult.ru/media/2022/10/27/1286894904/2017cifrovoe_pokolenie_rossii_compressed.pdf (дата обращения: 04.09.2024).

[11] Об информации, информационных технологиях и о защите информации : федер. закон от 27.07.2006 г. № 149-ФЗ [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/c5051782233acca771e9adb35b47d3fb82c9ff1c/ (дата обращения: 03.09.2024).

настроек конфиденциальности, местоположения и др. Необходимо осознать проблемы, понять последствия размещения своих данных и контента в социальных сетях и на иных цифровых платформах [21]. Однако «неподготовленные, недееспособные участники интернет-отношений (например, дети, пожилые люди и др.) не в состоянии сделать осознанный выбор и действовать для защиты своего личного пространства» [22].

Ж. Бодрийяр зафиксировал начало «экстаза коммуникации», эпохи «видимого, слишком видимого, более видимого, чем видимое»[12], когда понятие «социальная сеть» применялось для обозначения образа социальной структуры как системы взаимосвязанных точек или узлов. По мнению Ю. Хабермаса, современные социальные сети представляют собой перекресток, на котором сталкиваются пространства частного и приватного[13]. Важно понимать, когда пользователи делятся личной информацией, под адресатами своих информационных мессенджей они понимают круг людей, с которыми вступили в сетевые отношения, т. е. «друзей». В действительности они предоставляют данные «миру и городу», которые впоследствии могут использоваться третьими лицами в различных целях.

Ш. Теркл считает, что это ведет к иллюзии приватности, когда пользователи могут чувствовать себя защищенными в виртуальном мире, не осознавая реальных рисков и угроз нарушения их конфиденциальности, пребывая в уверенности, что личная информация доступна ограниченному числу людей[14]. Существуют механизмы защиты профиля в социальных сетях, например, сделать его полностью закрытым, использовать псевдонимы и др. Однако люди редко пользуются этими механизмами по ряду причин: отсутствие понимания уровня рисков, недостаточно умений работать с настройками социальных сетей, нежелание тратить время и силы на минимизацию рисков, ожидание от человека определенных действий по поддержанию отношений, формирование скептического отношения к принимаемым мерам [23].

Если подростки учитывают предупреждения о защите данных и предпринимают соответствующие действия (устанавливают надежные пароли, блокирующее рекламу программное обеспечение и др.), это не гарантирует защиту конфиденциальности и может формировать ложное чувство безопасности и иллюзию приватности[15]. Как отмечает д. бойд, подростки не всегда правильно оценивают социальные издержки, несмотря на постоянные мысли о них[16]. Для несовершеннолетних характерна низкая осведомленность о коммерческом сборе данных и персонифицированной рекламе, вследствие чего они придерживаются неполных или неточных убеждений, влияющих на поведение в интернете [24].

Многочисленные исследования отношения к конфиденциальности среди школьников и студентов свидетельствуют о наличии «парадокса конфиденциальности», фиксирующего расхождение между выраженной озабоченностью и реальным поведением пользователей. Систематический обзор литературы по этому вопросу показал, что процесс принятия пользователем решения о готовности разглашать конфиденциальную информацию определяется оценкой соотношения риска и пользы, нулевого или незначительного риска [25]. Беспечное отношение подростков к рискам определяется превалированием потребности во внимании и символического капитала,

[12] Baudrillard J. The Ecstasy of Communication. New York : Autonomedia, 1988. 107 p.

[13] Хабермас Ю. Новая структурная трансформация публичной сферы и делиберативная политика. М. : Новое литературное обозрение, 2023. 104 с.

[14] Turkle S. Alone Together: Why We Expect More from Technology and Less from Each Other. New York : Basic Books, 2012. 384 p. URL: https://www.mediastudies.asia/wp-content/uploads/2017/02/Sherry_Turkle_Alone_Together.pdf (дата обращения: 04.05.2024).

[15] Are We Living in Surveillance Societies and Is Privacy an Illusion? An Empirical Study on Privacy Literacy and Privacy Concerns / Ch. Prince [и др.] // IEEE Transactions on Engineering Management. 2021. Vol. 70, issue 10. p. 3553–3570. http://dx.doi.org/10.1109/TEM.2021.3092702

[16] бойд д. Все сложно. Жизнь подростков в социальных сетях. М. : Издательский дом Высшей школы экономики, 2020. 440 с.

который они получают через раскрытие персональной информации [26], над соображениями безопасности[17]. Подростки пренебрежительно относятся к рекомендациям родителей, учителей или любых других взрослых в связи с неопределенностью потенциального вреда [27; 28]. Цифровые аборигены не уверены в том, что происходит с их данными, говорят о невозможности их контроля, недоверии к крупным технологическим компаниям и непрозрачности современных систем обеспечения сохранности информации [29].

Для изменения ситуации необходимо переосмыслить проблему конфиденциальности в цифровом мире. Предпринимаемые усилия приносят определенные результаты: исследование итальянских ученых показало понимание подростками конфиденциальности в качестве морального и правового императива, основанного на взаимном уважении, который регулирует поведение людей в интернете [30]. Однако в этой работе изучается степень осознанного отношения подростков к цифровой безопасности и защите персональных данных, а не частота возникновения конкретных рисков.

Анализ проблемы цифровой безопасности подростков сопряжен со следующими трудностями: динамикой цифровой среды, непредсказуемостью угроз конфиденциальности, возникающих с появлением новых цифровых инструментов, реакцией подростков на эти угрозы. Несмотря на большое количество опубликованных исследований по теме, остаются нерешенными вопросы отношения подростков к использованию своих данных для обучения больших языковых моделей, свободного распространения чувствительных данных чат-ботам на основе больших языковых моделей, эффективности стратегий защиты персональных данных в этом случае.

[17] Slade S., Prinsloo P., Khalil M. Learning Analytics at the Intersections of Student Trust, Disclosure and Benefit // Proceedings of the 9th International Conference on Learning Analytics and Knowledge (LAK19). New York : Association for Computing Machinery, 2019. p. 235–244. https://doi.org/10.1145/3303772.3303796

Материалы и методы

В основе статьи лежат результаты социологического исследования «Кому принадлежат мои персональные данные?», проведенного коллективом авторов в конце 2023 – начале 2024 гг. на территории двух российских регионов: Республики Мордовия и Донецкой Народной Республики. Выборка квотная, репрезентует каждый из субъектов в отдельности по следующим признакам: пол, класс обучения. В нее вошли учащиеся 8–11 классов общеобразовательных школ. Соотношение юношей и девушек в каждом из регионов составило 46 на 54 % соответственно, доли учащихся 8-го класса – 35 %, 9-го – 36, 10-го – 15, 11-го – 14 %. Для повышения релевантности, полученный массив перевзвешен в соответствии с данными ведомственной статистики. Объем выборочной совокупности в каждом из двух исследуемых субъектов составил 300 чел. Погрешность исследования данной неслучайной выборки является аналитической, находится на уровне 5,5 %.

Сбор данных осуществлялся посредством Google Forms по стандартизированной интерактивной анкете. Перед ее заполнением опрошенные информировались о целях исследования, подтверждали факт согласия на участие в опросе и обработку полученных от них сведений.

Обработка данных проводилась в программе IBM SPSS Statistics 26, применены методы описательной и многомерной статистики. Разработанный инструментарий содержал индикаторы для выявления отношения подростков к сбору персональных данных, определения основного набора действий по обеспечению своей информационной безопасности. В инструментарии заложены три переменные: цифровые риски, цифровые последствия и цифровые меры безопасности. Каждой из них соответствуют 1–2 вопроса, анализируемые во взаимосвязи с независимыми индикаторами «пол», «класс обучения» и «место проживания»; дополнительно тестировалась декларируемая успеваемость школьников. Последняя переменная трактуется как значимая при исследовании навыков работы с цифровым контентом среди школьников, однако может осциллировать от позитивного к негативному

уровню воздействия в зависимости от методологической рамки [31].

Выбранные для сопоставления территории характеризуются тем, что Республика Мордовия – «старый» российский регион, где ряд показателей, за исключением объективных показателей благосостояния, приближен к общенациональным значениям[18]; Донецкую Народную Республику можно обозначить как новый российский регион, который слабо изучен социологами и не сравнивался с другими субъектами РФ. В первом случае можно говорить о типовом характере получаемых данных касаемо социально-политических вопросов, во втором – о «черном ящике», который необходимо расшифровать.

Проблемы обеспечения устойчивого интернета на территории «новых» регионов, качественного цифрового образовательного контента[19], могут порождать ситуацию цифрового неравенства. Подростки с ограниченным доступом к цифровой среде обладают меньшими компетенциями в сфере цифровой безопасности и защиты своих персональных данных и контента. Для проверки данной гипотезы необходимо сопоставить представления о цифровой безопасности у школьников из «нового» и типичного «старого» региона.

Результаты исследования

Проведенное исследование демонстрирует высокий уровень тревожности подростков относительно защиты своих персональных данных: 47 % опрошенных испытывают беспокойство, которое не зависит от территории проведения опроса (табл. 1). Статистически значимых корреляций относительно независимых переменных (пол, возраст, класс обучения, успеваемость) не обнаружено в обеих выборках. Наблюдается высокий уровень общей тревожности в Донецкой Народной Республике, что, по всей видимости, связано с нестабильной обстановкой ввиду непосредственной близости к передовой специальной военной операции. Известны случаи прямых угроз информационной безопасности жителей новых регионов, связанных с несанкционированным сбором их персональных данных через регистрацию на фейковых сайтах[20].

Подростки не испытывают оптимизма относительно сбора размещаемых ими данных на страницах социальных сетей, пользовательских комментариев для обучения машинных алгоритмов: 43 % опрошенных относятся отрицательно к подобным практикам, 31 % – затрудняются с ответом. Однако 26 % респондентов находят определенные плюсы – такие ответы детерминированы установкой на отсутствие угрозы для их информационной безопасности размещения пользовательского контента (табл. 2). Для технически продвинутых подростков это осознанная позиция: предоставление своих данных, контента для машинного обучения и разработки полезных цифровых инструментов – вклад в общее благо. Авторы исследований отмечают, что «увеличение погруженности в интернет не несет угрозы ощущению общественной и личной безопасности, если пользователь-подросток считает себя достаточно компетентным» [32]. Значимой социально-демографической характеристикой считается повышение доли положительных ответов юношей (33 % против 21 % девушек). Мнения подростков из Донецкой Народной Республики по поводу использования личных данных из социальных сетей пессимистичны. Разница позитивных и негативных ответов составляет – 24 процентных пункта (вдвое выше аналогичного показателя в Республике Мордовия), что свидетельствует о наличии региональных различий.

[18] Республика Мордовия глазами социологов : научный справочник ; под ред. В. В. Конакова, Е. А. Демьянова. Саранск : Научный центр социально-экономического мониторинга, 2017. 288 с. EDN: ZILNST

[19] В апреле 2024 г. в ДНР утверждена стратегия цифровой трансформации региона, в которой обозначена проблема низкого уровня использования учащимися цифровых устройств для образовательных целей. Об утверждении Стратегии в области цифровой трансформации отраслей экономики, социальной сферы и государственного управления Донецкой Народной Республики : Указ Главы Донецкой Народной Республики от 29.12.2023 г. № 644 [Электронный ресурс]. URL: http://publication.pravo.gov.ru/document/8000202401040014 (дата обращения: 03.09.2024).

[20] Киев создал сайт для сбора данных о жителях Республики, заявили в ЛНР [Электронный ресурс] // РИА Новости : офиц. сайт. URL: https://ria.ru/20191204/1561958267.html (дата обращения: 24.09.2024).

Таблица 1. **Распределение ответов на вопрос «Если говорить в целом, Вы испытываете или нет беспокойство по поводу конфиденциальности Ваших персональных данных?»,** % от общего числа опрошенных

Table 1. **Distribution of answers to the question "Are you concerned about the privacy of your personal data?",** % of the total number of respondents

Ответы респондентов / Respondents' answers	Все / Total	Республика Мордовия / Republic of Mordovia	Донецкая Народная Республика / Donetsk People's Republic
Безусловно испытываю / I definitely feel anxious	18	16	21
Скорее испытываю / I rather feel anxious	29	29	28
Скорее не испытываю / I rather do not feel anxious	31	36	26
Совсем не испытываю / I definitely don't feel anxious	13	11	14
Затрудняюсь ответить / I find it difficult to answer	9	8	11
Итого / Total	100	100	100

Примечание: здесь и далее в таблицах цветом выделены значения, превышающие аналогичный показатель в сопоставимом регионе.
Note: Hereinafter in tables values that exceed the same indicator in the comparable region are highlighted in color.

Источник: здесь и далее в статье все таблицы составлены авторами.
Source: Hereinafter in this article all tables were drawn up by authors.

Таблица 2. **Распределение ответов на вопрос «Как Вы относитесь к тому, что размещаемые Вами данные о себе в социальных сетях, Ваши пользовательские комментарии могут использоваться чат-ботами с искусственным интеллектом для обучения машинных алгоритмов?»,** % от общего числа опрошенных

Table 2. **Distribution of answers to the question "How do you feel about the fact that the information you post on social networks can be used by artificial intelligence chatbots to train machine algorithms?",** % of the total number of respondents

Ответы респондентов / Respondents' answers	Все / Total	Республика Мордовия / Republic of Mordovia	Донецкая Народная Республика / Donetsk People's Republic
Безусловно положительно / I am definitely positive	6	8	5
Скорее положительно / I have a rather positive attitude	20	23	16
Скорее отрицательно / I have a rather negative attitude	32	34	30
Определенно отрицательно / I am definitely negative	11	8	15
Затрудняюсь ответить / I find it difficult to answer	31	27	34
Итого / Total	100	100	100

Главные опасения подростков связаны с возможностью использования персональных данных в преступных целях (67 %), потери денег с банковской карты, финансовых потерь в целом (59 %), взлома страницы в социальных сетях, доступа к сообщениям в мессенджере (58 %), опасности для семьи, близких (57 %) и вторжения в личную жизнь, предания ее огласке (53 %) (табл. 3). Различия между двумя регионами в частоте разговоров относительно возможности финансовых потерь (66 % в Республике Мордовия против 51 % в Донецкой Народной Республике) объясняются меньшей

Таблица 3. **Распределение ответов на вопрос «Каких последствий Вы опасаетесь больше всего в случае использования Ваших персональных данных?»,** % от общего числа опрошенных

Table 3. **Distribution of answers to the question "What consequences do you most fear if your personal data is used?",** % of the total number of respondents

Ответы респондентов / Respondents' answers	Все / Total	Республика Мордовия / Republic of Mordovia	Донецкая Народная Республика / Donetsk People's Republic
Использование персональных данных в преступных целях / Use of personal data for criminal purposes	67	70	64
Потеря денег с банковской карты, финансовые потери в целом / Loss of money from a bank card, financial losses in general	59	66	51
Взлом страницы в социальных сетях, доступ к сообщениям в мессенджере / Hacking a page on social networks, accessing messages in the messenger	58	57	60
Опасность для семьи, близких / Danger to family and loved ones	57	56	58
Вторжение в личную жизнь, предание ее огласке / Invasion of privacy, making it public	53	53	52
Потеря важной информации / Loss of important information	47	42	51
Рекламные звонки, спам / Advertising calls, spam	23	23	22
Не опасаюсь последствий / I'm not afraid of the consequences	5	6	5
Затрудняюсь ответить / I find it difficult to answer	6	7	5
Итого / Total	375	380	368

распространенностью на «новых» территориях безналичных способов оплаты (точные данные отсутствуют, поэтому следует оставить это предположение в качестве гипотезы для последующих исследований).

Несмотря на распространенность рекламных обзвонов, около 23 % респондентов отметили обеспокоенность данным форматом несанкционированного использования персональных данных, что связано с увеличением масштабов утечки телефонных номеров. Появились способы надежной защиты от телефонного спама в виде автоматической блокировки нежелательных звонков или определителей номера. Исследование Д. В. Руденкина показало дисбаланс в использовании цифровой компетентности – молодые люди научились защищать себя от очевидных рисков стать жертвой мошенничества, однако «проявляют беспечность при следовании другим правилам, которые могут быть не менее важными в контексте обеспечения безопасности человека в информационном обществе» [28].

Проведенный корреляционный анализ демонстрирует незначительное повышение восприятия рисков потери денег с банковской карты, финансовых потерь в целом по мере увеличения возраста (r-Пирсона = 0,111 при $p \leq 0{,}01$); важность для девушек взлома страницы в социальных сетях, доступа к сообщениям (r-Пирсона = 0,146 при $p \leq 0{,}01$). Другие переменные не обладают статистической значимостью. Первая корреляция объясняется возможностью подростков с увеличением возраста получать собственные доходы и управлять ими. Болезненное отношение девушек к взлому аккаунтов в социальных сетях и мессенджерах связано с феноменом публичной интимности, «которая базируется на стремлении освободиться от жесткого

контроля со стороны значимых взрослых» [33] и выражается в форме визуального и текстового эпатажа. Несмотря на смелые репрезентации в социальных сетях и мессенджерах, девушки-подростки в личной переписке могут быть ближе к своей реальной личности, которую не хотят открывать для публичного доступа. Девушки чаще подвергаются насилию, издевательствам, сексуальным домогательствам в Сети [34], а риск перехода ненормативного общения из Сети в аналоговое пространство возрастает в случае потери данных из-за взлома аккаунта.

Ключевым механизмом защиты конфиденциальности большинство опрошенных подростков называют непредоставление своих персональных данных без веской причины (75 %). Показатели практически идентичны на территории обоих рассматриваемых субъектов. Частота выбора этого ответа повышается с классом обучения (с 68 % в 8 классе до 78 % в 11 классе), по мере роста успеваемости (с 68 % у троечников до 81 % у отличников).

Подобная тактика – пассивный способ обеспечения информационной безопасности. Переход к активным действиям декларирует 27 % опрошенных, 18 % из которых отключают гаджеты от сети, 12 % – заклеивают камеры. Только 9 % подростков не предпринимает никаких мер по обеспечению своей информационной безопасности, 12 % – затрудняются с ответом (табл. 4). Эти показатели перекликаются с исследованиями, проведенными в Томске и Томской области, где выявлено, что каждый пятый опрошенный школьник и учащийся СПО (20 и 19 % соответственно) обладает навыками киберприватности, к которым авторы относят умение создавать надежные пароли, использовать антивирусные программы и регулировать настройки приватности в социальных сетях [35]. Похожие результаты получены в ходе исследований молодежи Екатеринбурга, где большинство респондентов (82 %) декларируют высокий уровень уверенности в способности обеспечить надлежащий уровень своей информационной безопасности [28].

Варианты ответов настоящего исследования формулировались с учетом развития больших языковых моделей. Для обучения таких моделей требуется большой объем данных, чтобы они могли генерировать ответы на естественном языке. IT-компании используют доступные данные, включая публикации в социальных сетях. Персональные данные могут быть загружены на этапе использования чат-ботов на основе больших языковых моделей. Поэтому адекватным способом защиты персональных данных в этом случае является сокращение случаев их предоставления. Сложные пароли, антивирусные программы, обновление программного обеспечения и прочие привычные способы защиты личной информации могут быть недостаточно эффективными.

Полученные результаты свидетельствуют о частичном подтверждении первой исследовательской гипотезы, о полном – второй. Выявлены корреляции между полом и успеваемостью респондентов, случаи наибольшего опасения утечки персональных данных и способы защиты конфиденциальности.

Обсуждение и заключение

В процессе решения исследовательских задач и проверки гипотез установлено следующее.

Во-первых, отношение российских подростков к собственной информационной безопасности и конфиденциальности персональных данных амбивалентно: доли проявляющих беспокойство относительно персональных данных и тех, кто не беспокоится, одинаковы в структуре выборки. Большинство отрицательно относится к попаданию данных и размещаемого в социальных сетях контента в большие наборы данных, к применению для обучения нейросетей. Среди респондентов вызывает опасение возможность использования их данных в преступных целях, что не является прямым доказательством, однако косвенно свидетельствует о необоснованности предположения об иллюзии приватности, которая обнаруживается в ряде западных исследований.

Во-вторых, российские подростки испытывают чувство незащищенности при нахождении в виртуальном

Таблица 4. **Распределение ответов на вопрос «Скажите, Вы предпринимали какие-то меры для защиты своей конфиденциальности и персональных данных, и если да, то какие?»,** % от общего числа опрошенных

Table 4. **Distribution of answers to the question "Have you taken any measures to protect your confidentiality and personal data, and if yes, what were they?",** % of the total number of respondents

Ответы респондентов / Respondents' answers	Все / Total	Республика Мордовия / Republic of Mordovia	Донецкая Народная Республика / Donetsk People's Republic
Никому не предоставляю свои персональные данные, кроме случаев, когда без этого нельзя / I do not provide my personal data to anyone, except in cases when it is impossible without it	75	75	74
Беспокоюсь о конфиденциальности, но что-либо предпринимать мне лень / I'm worried about privacy, but I'm too lazy to do anything	20	23	17
Отключаю гаджеты от сети, когда не пользуюсь ими / I unplug gadgets when I'm not using them	18	15	21
Заклеиваю камеры в гаджетах / I tape cameras in gadgets	12	12	11
Другое / Other	1	1	1
Не предпринимаю никаких мер / I'm not taking any measures	9	7	11
Затрудняюсь ответить / I find it difficult to answer	11	13	10
Итого / Total	146	146	146

пространстве, которое может «трансгрессировать» в пространство реального (и наоборот). 12 % опрошенных не испытывают беспокойства насчет своей конфиденциальности и положительно относятся к использованию размещаемой ими информации для машинного обучения, что связано с беспечным отношением к своей информационной безопасности и осознанной позицией относительно необходимости вклада в общее благо в формате безвозмездного предоставления своих данных для развития полезных информационных инструментов. Противоположного мнения придерживаются 24 % респондентов, 60 % – опасаются того или иного аспекта сбора данных, 4 % – не могут ответить на поставленные вопросы.

В-третьих, преобладание юношей в числе тех, кто положительно относится к сбору данных для обучения нейросетей (33 % против 21 % среди девушек) соответствует общероссийским тенденциям: мужчины больше знают о нейросетях, чем женщины (17 % и 7 % соответственно). Положительное отношение к нейросетям характерно для тех, кто знаком с этой технологией (63 % технооптимистов среди разбирающихся в нейросетях против 21 % плохо осведомленных технопессимистов)[21]. Сравнение двух российских регионов – «старого» и «нового» – показывает смещение вектора в Республике Мордовия в сторону технооптимизма, в Донецкой Народной Республике чаще встречается цифровая незащищенность подростков. В данном случае необходимы дополнительные компаративистские исследования проблемы цифровой безопасности подростков из других субъектов Российской Федерации. В будущем необходимо использовать качественные методики (фокус-группы, глубинные интервью) для оценки причин и факторов восприятия нейросетей.

В-четвертых, несмотря на отсутствие иллюзии приватности, российские подростки не рефлексируют по поводу

[21] Нейросети и человек: начало пути [Электронный ресурс] // ВЦИОМ : офиц. сайт. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/neiroseti-i-chelovek-nachalo-puti (дата обращения: 02.09.2024).

загружаемой ими информации, недостаточно понимают корреляцию между персональными данными и пользовательским контентом. Относительно новой угрозы информационной безопасности, связанной с появлением нейросетей, совместной задачей родителей, школы, социальных сетей и правительственных учреждений должно стать комплексное разъяснение молодым людям опасностей утраты контроля над любыми данными, которое необходимо проводить в контексте повышения медиаграмотности и преодоления возникающих в обществе моральных паник [36].

В-пятых, анализ угроз использования данных несовершеннолетних в цифровом пространстве показал опасения относительно применения персональных данных в преступных целях. Такая тенденция наблюдается вне зависимости от региона проживания. Вторая беспокоящая подростков угроза – финансовые потери – волнует школьников Республики Мордовия, что, по всей видимости, связано с меньшей распространенностью финансовых онлайн-услуг и безналичных способов оплаты в Донецкой Народной Республике. Доминирующие способы обеспечения цифровой безопасности носят пассивный характер, ограничиваясь декларацией беспокойства, что не зависит от места проживания опрашиваемых подростков. Грамотной стратегией в условиях сбора больших данных является отказ от предоставления информации, кроме случаев необходимости. Такой вариант поведения чаще выбирают старшеклассники с высокой успеваемостью. Стратегии «защити себя сам» – выключение гаджетов из сети, заклеивание камер – пока находятся в меньшинстве, указывая на наличие доминирующего внутреннего локуса контроля [37]. Остальным подросткам требуется внешняя мотивация для защиты своей персональной информации.

Таким образом, изучение факторов активной позиции подростков по обеспечению собственной цифровой безопасности представляется перспективной научной задачей, отправной точкой для решения которой могут стать полученные результаты данной статьи, отражающие текущий уровень восприятия рисков и угроз публичного размещения персональных данных и контента в социальных сетях. Выдвинутая гипотеза о беспечном отношении подростков к размещению своих персональных данных и использованию их контента для машинного обучения подтвердилась частично. Вторая гипотеза о различиях в уровне тревожности относительно пользовательских данных подростков из «старого» и «нового» российских регионов подтвердилась полностью, однако необходимо подчеркнуть небольшую величину этих различий.

Рекомендации для повышения цифрового суверенитета подростков основываются на Концепции информационной безопасности детей, однако авторами добавлены принципиальные уточнения, связанные с изменением подходов к оценке рисков в сфере цифровой безопасности после появления общедоступных чат-ботов на основе больших языковых моделей:

1. Провести ревизию действующих образовательных программ на предмет содержания в них основ информационной безопасности. Помощь в освоении виртуального пространства должна быть включена в образовательный минимум на этапе младшей школы, когда ребенок начинает активно осваивать смартфон.

2. Интегрировать в учебный процесс модули информационной грамотности и цифровой безопасности детей: в формате теории будут рассматриваться риски неправильного обращения со своими данными и разбираться отдельные кейсы. Необходимо сделать упор на механизмах защиты школьников в виртуальном пространстве при использовании чат-ботов на основе больших языковых моделей. Речь идет о модульном подходе внедрения отдельных тем или тематических блоков в существующие образовательные курсы (информатика, основы безопасности и защиты Родины, технология (труд), обществознание и др.) и/или внеурочные занятия (разговоры о важном, 36 уроков будущего отличника и др.), а не о введении новых предметов и дисциплин в ущерб имеющимся.

3. Систематически проводить просветительские мероприятия по темам основ информационной грамотности

и цифровой безопасности детей в условиях постоянного накопления больших данных, развития больших языковых моделей и чат-ботов на их основе, ориентированные на подростков и их родителей (законных представителей), работников системы образования и специалистов по внеучебной работе.

4. Разработать и реализовать оценку цифровых компетенций населения нашей страны с основой на индексном подходе (например, «Индекс информационной грамотности и цифровой безопасности»), которая позволит сравнивать между собой уровни знаний, навыков и установок в российских регионах, внутри различных социальных групп с обязательным выделением младших, средних и старших школьников. Количественные методики измерения информационной грамотности необходимо дополнить качественными инструментами (фокус-группами, глубинными интервью), объясняющими причинность измеряемых явлений и процессов, добавить исследовательской глубины.

Полученные в ходе исследования данные расширяют научные представления о процессах восприятия цифровой безопасности среди российских подростков. Дальнейшее изучение этого вопроса необходимо сосредоточить в направлении анализа причин стратегий противодействия внешним угрозам, в том числе мотивов полагания на внешний или внутренний локус контроля, которые могут быть выявлены посредством качественных методов. Материалы настоящего исследования будут интересны специалистам по вопросам цифровой безопасности, сотрудникам органов государственной власти и местного самоуправления, разрабатывающим комплексные решения формирования системы информационной безопасности детей и молодежи.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

1. Гуркина О.А., Мальцева Д.В. Мотивы использования виртуальных социальных сетей подростками. *Социологические исследования.* 2015;(5):123–130. URL: https://www.socis.isras.ru/article/5226 (дата обращения: 19.06.2024).
   Gourkina O.A., Maltseva D.V. [Adolescents' Motivations to Use Virtual Social Networking Sites]. *Sociological Studies*. 2015;(5):123–130. (In Russ.) Available at: https://www.socis.isras.ru/article/5226 (accessed 19.06.2024).
2. Barnes S.B. A Privacy Paradox: Social Networking in the United States. *First Monday*. 2006;11(9):1394. https://doi.org/10.5210/fm.v11i9.1394
3. Youn S. Parental Influence and Teens' Attitude toward Online Privacy Protection. *Journal of Consumer Affairs.* 2008;42(3):362–388. https://doi.org/10.1111/j.1745-6606.2008.00113.x
4. Мальцева Н.Н., Новак М.В. Медиаграмотность, безопасность и социализация личности в цифровом пространстве: обзор отечественной и зарубежной аналитики. *Научный результат. Социальные и гуманитарные исследования.* 2023;9(1):207–212. URL: https://rrhumanities.ru/journal/article/3027/ (дата обращения: 14.07.2024).
   Maltseva N.N., Novak M.V. Media Literacy, Security and Socialization of the Individual in the Digital Space: Overview Analytics. *Research Result. Social Studies and Humanities*. 2023;9(1):207–212. (In Russ., abstract in Eng.) Available at: https://rrhumanities.ru/journal/article/3027/ (accessed 14.07.2024).
5. Tomczyk Ł., Eger L. Online Safety as a New Component of Digital Literacy for Young People. *Integration of Education*. 2020;24(2):172–184. https://doi.org/10.15507/1991-9468.099.024.202002.172-184
6. Филиппов В.М., Насонкин В.В., Папачараламбоус Ч. Права и интересы детей в информационной сфере: реформирование законодательства. *Вестник Санкт-Петербургского университета. Право.* 2019;10(2):362–372. https://doi.org/10.21638/spbu14.2019.211
   Filippov V.M., Nasonkin V.V., Papacharalambous C. Rights and Interests of Children in the Information Sphere: Improvement of Legislation. *Vestnik of Saint-Petersburg University. Law*. 2019;10(2):362–372. (In Russ., abstract in Eng.) https://doi.org/10.21638/spbu14.2019.211
7. Young S. Zoombombing Your Toddler: User Experience and the Communication of Zoom's Privacy Crisis. *Journal of Business and Technical Communication*. 2020;35(1):147–153. http://dx.doi.org/10.1177/1050651920959201

8. Semantha F.H., Azam S., Shanmugam B., Yeo K.C. PbDinEHR: A Novel Privacy by Design Developed Framework Using Distributed Data Storage and Sharing for Secure and Scalable Electronic Health Records Management. *Journal of Sensor and Actuator Networks*. 2023;12(2):36. https://doi.org/10.3390/jsan12020036
9. Ушкин С.Г. Практики сбора персональных данных и их восприятие в общественном сознании. *Вестник Томского государственного университета. Философия. Социология. Политология.* 2024;(77):251–261. URL: https://vital.lib.tsu.ru/vital/access/manager/Repository/koha:001145764?y=0&x=0 (дата обращения: 14.07.2024).
Ushkin S.G. Practices of Collecting Personal Data and Their Perception in the Public Consciousness. *Tomsk State University Journal of Philosophy, Sociology and Political Science.* 2024;(77):251–261. (In Russ., abstract in Eng.) Available at: https://vital.lib.tsu.ru/vital/access/manager/Repository/koha:001145764?y=0&x=0 (accessed 14.07.2024).
10. Солдатова Г.У., Теславская О.И. Персональные данные и дети: вопросы безопасности. *Эпоха науки.* 2017;(12):92–102. URL: http://eraofscience.com/EofS/Vypyski2017/December2017g/12-dekabr_2017_g..pdf#page=93 (дата обращения: 14.07.2024).
Soldatova G.U., Teslavskaya O.I. Personal Data and Children: Issues of Safety. *Epokha nauki*. 2017;(12):92–102. (In Russ., abstract in Eng.) Available at: http://eraofscience.com/EofS/Vypyski2017/December2017g/12-dekabr_2017_g..pdf#page=93 (accessed 14.07.2024).
11. Hoffmann A.L. Where Fairness Fails: Data, Algorithms, and the Limits of Antidiscrimination Discourse. *Information, Communication and Society*. 2019;22(7):900–915. https://doi.org/10.1080/1369118X.2019.1573912
12. Мухамадиева К.Б. Искусственный интеллект в развитии молодежи. *Образование и проблемы развития общества.* 2021;(2):27–33. EDN: DDJAGW
Mukhamadieva K.B. Artificial Intelligence in the Development of Youth. *Education and Problems of Development of Society*. 2021;(2):27–33. (In Russ., abstract in Eng.) EDN: DDJAGW
13. Медведева М.В. Риски использования нейросетевых технологий в коммуникациях молодежи. *Российская школа связей с общественностью.* 2023;(30):139–151. https://doi.org/10.24412/2949-2513-2023-30-139-151
Medvedeva M.V. Risks of Using Neural Network Technologies in Youth Communications. *Russian School of Public Relations.* 2023;(30):139–151. (In Russ., abstract in Eng.) https://doi.org/10.24412/2949-2513-2023-30-139-151
14. Hummel P., Braun M., Dabrock P. Own Data? Ethical Reflections on Data Ownership. *Philosophy and Technology*. 2021;34:545–572. https://doi.org/10.1007/s13347-020-00404-9
15. Маринова Е.В. Терминотворчество в русскоязычном дискурсе о «цифре». *Terra Linguistica*. 2023;14(3):61–79. https://doi.org/10.18721/JHSS.14306
Marinova E.V. Terms Creation in the Russian-Language Discourse on “Digit”. *Terra Linguistica*. 2023;14(3):61–79. (In Russ., abstract in Eng.) https://doi.org/10.18721/JHSS.14306
16. Бегишев И. Семантический анализ термина «цифровая безопасность». *Юрислингвистика.* 2021;(20):24–38. https://doi.org/10.14258/leglin(2021)2005
Begishev I. Semantic Analysis of the Term “Digital Security”. *Legal Linguistics*. 2021;(20):24–38. (In Russ., abstract in Eng.) https://doi.org/10.14258/leglin(2021)2005
17. Бороненко Т.А., Кайсина А.В., Федотова В.С. Развитие цифровой грамотности школьников в условиях создания цифровой образовательной среды. *Перспективы науки и образования.* 2019;(2):167–193. https://doi.org/10.32744/pse.2019.2.14
Boronenko T.A., Kaysina A.V., Fedotova V.S. The Development of Digital Literacy of Schoolchildren in Conditions of Creating a Digital Educational Environment. *Perspectives of Science and Education*. 2019;(2):167–193. (In Russ., abstract in Eng.) https://doi.org/10.32744/pse.2019.2.14
18. Пинкевич Т.В., Нестеренко А.В. Нарушение неприкосновенности частной жизни при использовании технологии «Больших данных». *Юридическая наука и практика: Вестник Нижегородской академии МВД России.* 2019;2019(3):143–147. https://doi.org/10.36511/2078-5356-2019-3-143-147
Pinkevich T.V., Nesterenko A.V. Violation of Privacy When Using Big Data Technologies. *Legal Science and Practice*: *Journal of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*. 2019;2019(3):143–147. (In Russ., abstract in Eng.) https://doi.org/10.36511/2078-5356-2019-3-143-147
19. Овчинников А.И., Ахрамеева О.В., Воронцов С.А., Кожокарь И.П., Кравченко А.Г., Мамычев А.Ю., и др. Цифровая безопасность личности, общества и государства в условиях глобализации: юридические механизмы обеспечения. Обзор сессии в рамках ПМЮФ 2019 г. *Вестник юридического факультета Южного федерального университета.* 2019;6(2):111–122. URL: https://urvestnikpravo.sfedu.ru/index.php/Vestnikurfaksfedu/issue/view/6 (дата обращения: 14.07.2024).

Ovchinnikov A.I., Akhrameeva O.V., Vorontsov S.A., Kozhokar I.P., Kravchenko A.G., Mamychev A.Yu., et al. Digital Security of the Individual, Society and the State in the Context of Globalization: Legal Mechanisms to Ensure. Overview of the Session within the Legal Forum Live Project of the St. Petersburg International Legal Forum 2019. *Bulletin of the Law Faculty, Southern Federal University*. 2019;6(2):111–122. (In Russ., abstract in Eng.) Available at: https://urvestnikpravo.sfedu.ru/index.php/Vestnikurfaksfedu/issue/view/6 (accessed 14.07.2024).

20. Селюнина С.В., Горбачева Н.А. Теоретические и практические аспекты обеспечения информационной безопасности детей и подростков в глобальной сети. *Здоровье населения и среда обитания.* 2017;(8):11–17. EDN: ZEVTPP
Selyunina S.V., Gorbacheva N.A. Theoretical and Practical Aspects of Ensuring Information Security of Children and Teenagers in Global Network. *Public Health and Life Environment*. 2017;(8):11–17. (In Russ., abstract in Eng.) EDN: ZEVTPP
21. Chang V., Golightly L., Xu Q.A., Boonmee T., Liu B.S. Cybersecurity for Children: An Investigation into the Application of Social Media. *Enterprise Information Systems*. 2023;17(11):2188122. https://doi.org/10.1080/17517575.2023.2188122
22. Самохина Н.Н. Безопасность личности в интернет-пространстве: установление и защита новых границ конфиденциальности. *Экономические и социально-гуманитарные исследования.* 2023;(1):148–154. URL: https://esgi-miet.ru/images/Stati20231/ESGI_2023_1-37_1.indd.pdf (дата обращения: 14.07.2024).
Samokhina N.N. Personal Security in the Internet Space: Establishing and Protecting New Boundaries of Privacy. *Economic and Social Research*. 2023;(1):148–154. (In Russ., abstract in Eng.) Available at: https://esgi-miet.ru/images/Stati20231/ESGI_2023_1-37_1.indd.pdf (accessed 14.07.2024).
23. Чеснокова Л.В. Размывание границы между публичностью и приватностью в социальных сетях и парадокс приватности. *Философские проблемы информационных технологий и киберпространства.* 2021;(2):22–38. https://doi.org/10.17726/philIT.2021.2.2
Chesnokova L.V. Blurring the Line between Publicity and Privacy on Social Media and the Privacy Paradox. *Philosophical Problems of IT and Cyberspace*. 2021;(2):22–38. (In Russ., abstract in Eng.) https://doi.org/10.17726/philIT.2021.2.2
24. Holvoet S., De Jans S., De Wolf R., Hudders L., Herrewijn L. Exploring Teenagers' Folk Theories and Coping Strategies Regarding Commercial Data Collection and Personalized Advertising. *Media and Communication*. 2022;10(1):317–328. https://doi.org/10.17645/mac.v10i1.4704
25. Barth S., de Jong M.D.T. The Privacy Paradox – Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review. *Telematics and Informatics*. 2017;34(7):1038–1058. https://doi.org/10.1016/j.tele.2017.04.013
26. Park Y.J. Digital Literacy and Privacy Behavior Online. *Communication Research*. 2013;40(2):215–236. https://doi.org/10.1177/0093650211418338
27. Wisniewski P. The Privacy Paradox of Adolescent Online Safety: A Matter of Risk Prevention or Risk Resilience? *IEEE Security and Privacy*. 2018;16(2):86–90. https://doi.org/10.1109/MSP.2018.1870874
28. Руденкин Д.В. Уровень развития навыков цифровой гигиены современной российской молодежи: итоги социологического исследования. *Социодинамика.* 2022;(1):36–55. https://doi.org/10.25136/2409-7144.2022.1.37487
Rudenkin D. The Level of Development of Digital Hygiene Skills of Modern Russian Youth: The Results Sociological Research. *Sociodynamics.* 2022;(1):36–55. (In Russ., abstract in Eng.) https://doi.org/10.25136/2409-7144.2022.1.37487
29. Maier E., Doerk M., Reimer U., Baldauf M. Digital Natives Aren't Concerned Much about Privacy, or Are They? *i-com*. 2023;22(1):83–98. https://doi.org/10.1515/icom-2022-0041
30. Vespoli G., Taddei B., Imbimbo E., De Luca L., Nocentini A. The Concept of Privacy in the Digital World According to Teenagers. *Journal of Public Health*. 2024. https://doi.org/10.1007/s10389-024-02242-x
31. Костина С.Н., Новикова О.Н. Как старшие подростки оценивают влияние цифровых технологий на учебную деятельность? *Вестник Томского государственного университета. Философия. Социология. Политология.* 2023;(74):190–205. EDN: JGXWML
Kostina S.N., Novikova O.N. Impact of Digital Technologies on Learning Activities of Adolescents. *Tomsk State University Journal of Philosophy, Sociology and Political Science*. 2023;(74):190–205. (In Russ., abstract in Eng.) EDN: JGXWML
32. Регуш Л.А., Алексеева Е.В., Веретина О.Р., Орлова А.В, Пежемская Ю.С. Психологические проблемы подростков и интернет-среда: диагностика и способы совладания. *Вестник Российского фонда фундаментальных исследований. Гуманитарные и общественные науки.*

2023;(3):72–85. URL: https://www.rfbr.ru/storage/library/vestnik/pdf/60ec69f0960d62e139cea159f61fdc2c.pdf (дата обращения: 14.07.2024).
Regush L.A., Alexeyeva E.V., Veretina O.R., Orlova A.V., Pezhemskaya Yu.S. Internet-Related Psychological Issues in Adolescents: Diagnosis and Coping Strategies. *Russian Foundation for Basic Research Journal. Humanities and Social Sciences*. 2023;(3):72–85. (In Russ., abstract in Eng.) Available at: https://www.rfbr.ru/storage/library/vestnik/pdf/60ec69f0960d62e139cea159f61fdc2c.pdf (accessed 14.07.2024).

33. Каркищенко Е.А. Анкетные данные в социальной сети как репрезентация гендерной идентичности подростка. *Вестник Московского университета.* Сер. *9. Филология*. 2013;(3):160–167. URL: https://vestnik.philol.msu.ru/issues/VMU_9_Philol__2013_3.pdf (дата обращения: 25.02.2024).
Karkishchenko E.A. [Personal Questionnaire Data as Representation of a Teenager's Gender Identity]. *Moscow University Bulletin. Series 9. Philology*. 2013;(3):160–167. (In Russ., abstract in Eng.) Available at: https://vestnik.philol.msu.ru/issues/VMU_9_Philol__2013_3.pdf (accessed 25.02.2024).
34. Борисенко Е.В., Дозорцева Е.Г. Мотивационно-смысловые характеристики участия в секстинге несовершеннолетних девочек. *Психология и право.* 2023;13(3):3–15. https://doi.org/10.17759/psylaw.2023130301
Borisenko E.V., Dozortseva E.G. Motivation and Subjective Meaning of Participation in Sexting in Minor Girls. *Psychology and Law.* 2023;13(3):3–15. (In Russ., abstract in Eng.) https://doi.org/10.17759/psylaw.2023130301
35. Глухов А.П., Соломина И.Г. Факторы киберсоциализации и цифровая грамотность обучающихся. *Вестник Томского государственного университета. Философия. Социология. Политология.* 2024;(78):146–156. EDN: ETWKAM
Glukhov A.P., Solomina I.G. Factors of Cybersocialization and Digital Literacy of Students. *Tomsk State University Journal of Philosophy, Sociology and Political Science*. 2024;(78):146–156. (In Russ., abstract in Eng.) EDN: ETWKAM
36 De Leyn T., Waeterloos C., De Wolf R., Vanhaelewyn B., Ponnet K., De Marez L. Teenagers' Reflections on Media Literacy Initiatives at School and Everyday Media Literacy Discourses. *Journal of Children and Media*. 2021;16(2):221–239. https://doi.org/10.1080/17482798.2021.1952463
37. Whelan E., Lang M., Butler M. Beyond Lazy; External Locus of Control as an Alternative Explanation for the Privacy Paradox. *Internet Research*. 2024;35(1):349–379. https://doi.org/10.1108/INTR-04-2023-0282

Об авторах:

Ушкин Сергей Геннадьевич, кандидат социологических наук, ведущий научный сотрудник Научного центра социально-экономического мониторинга (430005, Российская Федерация, г. Саранск, ул. Б. Хмельницкого, д. 39а), исследовательский менеджер Всероссийского центра изучения общественного мнения (119034, Российская Федерация, г. Москва, ул. Пречистенка, д. 38), младший научный сотрудник МГУ им. Н. П. Огарёва (430005, Российская Федерация, г. Саранск, ул. Большевистская, д. 68), **ORCID: https://orcid.org/0000-0003-4317-6615**, **Scopus ID: 55489629800**, **Researcher ID: E-7455-2017, SPIN-код: 1894-6660**, ushkinsergey@gmail.com

Коваль Екатерина Александровна, доктор философских наук, профессор кафедры уголовного права и процесса Средне-Волжского института (филиала) ВГУЮ (РПА Минюста России) (430003, Российская Федерация, г. Саранск, ул. Федосеенко, д. 6), профессор кафедры всеобщей истории, политологии и регионоведения МГУ им. Н. П. Огарёва (430005, Российская Федерация, г. Саранск, ул. Большевистская, д. 68), **ORCID: https://orcid.org/0000-0003-0069-5335**, **Scopus ID: 57202425856**, **Researcher ID: A-5797-2015**, **SPIN-код: 7939-4818**, nwifesc@yandex.ru

Мартынова Марина Дмитриевна, кандидат философских наук, доцент МГУ им. Н. П. Огарёва (430005, Российская Федерация, г. Саранск, ул. Большевистская, д. 68), **ORCID: https://orcid.org/0000-0003-1244-9721**, **Scopus ID: 57225145640**, **Researcher ID: HKN-1837-2023**, **SPIN-код: 1287-0833**, martynovamd@mail.ru

Заявленный вклад авторов:

С. Г. Ушкин – разработка концепции исследования; визуализация результатов исследования; написание черновика рукописи.

Е. А. Коваль – разработка методологии исследования; проведение исследования; критический анализ черновика рукописи.

М. Д. Мартынова – управление планированием и проведением исследования; написание черновика рукописи, критический анализ черновика рукописи.

Доступность данных и материалов. Набор данных, использованные и/или проанализированные в ходе текущего исследования, можно получить у авторов по обоснованному запросу.

Все авторы прочитали и одобрили окончательный вариант рукописи.

Поступила 30.07.2024; одобрена после рецензирования 04.10.2024; принята к публикации 11.10.2024.

About the authors:

Sergey G. Ushkin, Cand.Sci. (Sociol.), Leading Researcher, Scientific Center for Socio-Economic Monitoring (39a B. Khmelnitskogo St., Saransk 430005, Russian Federation), Research Manager, Russian Public Opinion Research Center (38 Prechistenka St., Moscow 119034, Russian Federation), Researcher, National Research Mordovia State University (68 Bolshevistskaya St., Saransk 430005, Russian Federation), **ORCID: https://orcid.org/0000-0003-4317-6615**, **Scopus ID: 55489629800**, **Researcher ID: E-7455-2017**, **SPIN-code: 1894-6660**, ushkinsergey@gmail.com

Ekaterina A. Koval, Dr.Sci. (Philos.), Professor, Chair of Criminal Law and Criminal Procedure, Middle Volga Branch, All-Russian State University of Justice (6 Fedoseenko St., Saransk 430003, Russian Federation), Professor, Chair of General History, Political Science and Area Studies, National Research Mordovia State University (68 Bolshevistskaya St., Saransk 430005, Russian Federation), **ORCID: https://orcid.org/0000-0003-0069-5335**, **Scopus ID: 57202425856**, **Researcher ID: A-5797-2015**, **SPIN-code: 7939-4818**, nwifesc@yandex.ru

Marina D. Martynova, Cand.Sci. (Philos.), Associate Professor, National Research Mordovia State University (68 Bolshevistskaya St., Saransk 430005, Russian Federation), **ORCID: https://orcid.org/0000-0003-1244-9721**, **Scopus ID: 57225145640**, **Researcher ID: HKN-1837-2023**, **SPIN-code: 1287-0833**, martynovamd@mail.ru

Authors' contribution:

S. G. Ushkin – development of the research concept; visualization, analysis and interpretation of research results; preparation of the initial version of the manuscript.

E. A. Koval – development of sociological research tools; data collection; revision of the manuscript.

M. D. Martynova – organization of sociological research; data collection; revision of the manuscript.

Availability of data and materials. The datasets used and/or analyzed during the current study are available from the authors on reasonable request.

All authors have read and approved the final manuscript.

Submitted 30.07.2024; revised 04.10.2024; accepted 11.10.2024.