

Научно-практическая статья  
УДК 004.056  
JEL classification: D83, O33  
EDN: YDJDLL

## ЦИФРОВАЯ ГРАМОТНОСТЬ КАК ОРУЖИЕ ПРОТИВ ИНФОРМАЦИОННОЙ ВОЙНЫ: ОБРАЗОВАНИЕ И ТЕХНОЛОГИИ ДЛЯ РАСПОЗНАВАНИЯ МАНИПУЛЯЦИЙ

**Саргсян А.П.,**

обучающийся бакалавриата кафедры маркетинга и логистики,  
Донецкий филиал РАНХиГС,  
г. Донецк, Донецкая Народная Республика, Российская Федерация.  
E-mail: annasarg2016@gmail.com

**Аннотация. Цель.** Обоснование роли цифровой грамотности как средства противостояния информационной войне. Определение компонентов цифровой грамотности, их влияние на критическое мышление. Предложение методов, стратегий повышения цифровой грамотности для защиты от дезинформации и укрепления безопасности.

**Материалы и методы.** Исследование основано на анализе научной литературы по цифровой грамотности, информационной войне, манипуляциям, а также обзоре образовательных программ, направленных на развитие критического мышления. Методология включает изучение нормативно-правовых актов, направленных на повышение цифровой грамотности и разбор механизмов воздействия социальных сетей, когнитивных искажений.

**Результаты.** Было установлено, что ключевыми компонентами цифровой грамотности, необходимые для противостояния информационной войне, выступают человеческие способности, такие как: развитие критического мышления, умение объективно оценивать источники информации, своевременное распознавание манипуляций и попыток формирования когнитивных искажений. Также подтверждена значимая роль образования и правового регулирования в повышении общей цифровой грамотности населения, создании информационно безопасной среды и формировании устойчивости к дезинформации. Кроме того, были выявлены эффективные методы и стратегии противодействия манипуляциям, распространяемым через социальные сети и другие медиаканалы, включая, тщательную проверку любых поступающих сведений и использование современных инструментов защиты информации. Наконец, акцентирована важность внедрения и широкого использования цифровых технологий, таких как электронные подписи и блокчейн, для целей верификации официального контента, защиты его от подделок и повышения общего уровня доверия к распространяемой информации.

**Заключение.** Результаты исследования подтверждают, что цифровая грамотность является необходимым условием для эффективного противостояния информационной войне и защиты граждан от деструктивных манипуляций. Реализация данного подхода позволит существенно укрепить информационную безопасность государства и сформировать общество, устойчивое к дезинформации и способное критически оценивать поступающую информацию. Данный вывод имеет практическую значимость для развития цифровой грамотности в контексте современного общества, требующей комплексного подхода, включающего образовательные инициативы, соответствующее правовое регулирование и активное внедрение передовых информационных технологий.

**Ключевые слова:** цифровая грамотность, информация, информационная война, цифровые технологии, коммуникации, манипуляции, безопасность.

**Для цитирования:** Саргсян А.П. Цифровая грамотность как оружие против информационной войны: образование и технологии для распознавания манипуляций. «Феноменус». 2026. №1(33). С. 132–138. EDN: YDJDLL



Scientific and practical article  
UDC 004.056  
JEL classification: D83, O33  
EDN: YDJDLL

## DIGITAL LITERACY AS A WEAPON AGAINST THE INFORMATION WAR: EDUCATION AND TECHNOLOGIES TO RECOGNIZE MANIPULATION

**Anna P. Sargsian,**

Bachelor's degree student of the Department of Marketing and Logistics,  
Donetsk Branch of RANEPА,  
Donetsk, Donetsk People's Republic, Russian Federation.  
E-mail: annasarg2016@gmail.com

**Annotation. Objective.** To justify the significance of digital literacy as a mean to counter the information war. To define the components of digital literacy and analyze their impact on the development of critical thinking skills, as well as proposing effective methods and strategies for enhancing digital literacy to safeguard against disinformation and strengthen overall information security.

**Materials and Methods.** The study is grounded in an analysis of scholarly literature pertaining to digital literacy, information warfare, and manipulative techniques. It also encompasses a review of educational programs designed to foster critical thinking skills. The methodology incorporates an examination of regulatory frameworks and legal instruments aimed at promoting digital literacy, alongside a dis-assembly of the mechanisms through which social media platforms and cognitive biases exert influence.

**Results.** The study revealed that key components of digital literacy, essential for countering information warfare, include human capacities such as the development of critical thinking, the ability to objectively evaluate information sources, and the timely recognition of manipulation and attempts to form cognitive biases. The significant role of education and legal regulation lies in improving overall digital literacy among the population, creating an information-secure environment, and fostering resilience to disinformation was also confirmed. Furthermore, effective methods and strategies for counteracting manipulations spread through social networks and other media channels were identified, including rigorous verification of any incoming information and the use of modern information protection tools. Finally, the importance of implementing and widely using digital technologies, such as electronic signatures and blockchain, for verifying official content, protecting it from falsification, and increasing the overall level of trust in the disseminated information was emphasized.

**Conclusion.** The research findings confirm that digital literacy is a necessary condition for effectively countering information warfare and protecting citizens from destructive manipulations. The implementation of this approach will significantly strengthen the information security of the country and form a society that is resistant to disinformation and capable of critically evaluating incoming information. Such a conclusion has practical significance for the development of digital literacy in the context of modern society, requiring a comprehensive approach that includes educational initiatives, appropriate legal regulation, and the active implementation of advanced information technologies.

**Keywords:** digital literacy, information, information warfare, digital technology, communication, manipulation, security.

**For citation:** Sargsian, A. P., (2026) Digital literacy as a weapon against the informational war: education and technologies to recognize manipulation. Phenomenus, 1(33), 132-138. EDN: YDJDLL

### Постановка проблемы в общем виде

В современном мире информационная война приобретает особенно острые формы через целенаправленные манипуляции медиаконтентом, распростра-

няющиеся с невероятной скоростью по социальным сетям и платформам, мгновенно искажая восприятие реальности у миллионов пользователей и систематически подрывая доверие к традиционным и независимым источникам



информации. Такие операции часто опираются на алгоритмы, усиливающие эмоционально заряженный контент, что приводит к вирусному эффекту и формированию ложных нарративов, способных влиять на общественное мнение, политические процессы и даже международные отношения. Цифровая грамотность (ЦГ) в этом контексте выступает как жизненно важный набор навыков критического мышления, позволяющий обычным пользователям не просто потреблять информацию в глобальной сети Интернет, но глубоко её анализировать: проверять факты на соответствие первоисточникам, оценивать авторитетность авторов и платформ, распознавать признаки манипуляции вроде селективных цитат или подтасованных данных, а также учитывать контекст и возможные скрытые мотивы.

Актуальность настоящего исследования обусловлена растущей сложностью и повсеместностью информационных войн в цифровую эпоху, что подчёркивает острую необходимость в населении, обладающем развитыми навыками цифровой грамотности. Определяя основные компетенции в области цифровой грамотности и изучая стратегии их совершенствования, данное исследование восполняет критический пробел в готовности общества к навигации по вызовам современной информационной среды, где особенно важна способность не просто потреблять контент, но глубоко его деконструировать, учитывая контекст создания, мотивы распространителей и потенциальные скрытые повестки.

#### **Цель исследования**

Цель исследования – определить и обосновать эффективные подходы к развитию цифровой грамотности как ключевого инструмента противодействия информационным войнам и манипуляциям.

Объект исследования – процессы влияния цифровых технологий на уровень цифровой грамотности населения и их способность противостоять информационным манипуляциям в современной информационной среде.

Предмет исследования – методы и технологии, применяемые для повышения критического мышления, навыков верификации информации и распознавания манипуляций, а также анализ их эффективности в контексте противодействия информационной войне.

#### **Изложение основного материала исследования**

Понятие «цифровая грамотность»

(DL, Digital Literacy) начало формулироваться в мире на стыке 1980–1990-х годов и вошло в широкое употребление с 1997 года, после выхода книги Пола Гилстера «Цифровая грамотность» [1]. П. Гилстер интерпретировал ЦГ как «способность понимать и использовать информацию в различных форматах из широкого спектра источников, представленных с помощью компьютера» [1, с. 1]. В России термин «цифровая грамотность» стал активно изучаться в научных публикациях с 2010 года и изначально его определяли как «грамотность в использовании современных технических цифровых средств» [2] и т. п.

С появлением цифровых технологий границы грамотности расширились. Осознание информации с экрана требует тех же когнитивных процессов, что и из печатных или телевизионных СМИ. В 2015 г. определение цифровой грамотности актуализировано в проекте «Индекс цифровой грамотности»: это комплекс знаний и навыков для безопасного и эффективного применения цифровых технологий и интернета, охватывающий потребление контента, ключевые компетенции и меры безопасности [3, с. 7]. Цифровую грамотность нередко сводят к одному из технических навыков – умению работать с гаджетами для решения повседневных задач. Однако интернет изначально создавался как платформа для общения, и эта функция остаётся его основной сутью. Сервисы (сообщения, социальные сети, форумы, блоги, комментарии) реализуют коммуникативные потребности пользователей. Следовательно, грамотность включает взаимодействие между людьми. Акцент на утверждении: «Цифровая грамотность – это способность использовать возможности общества с технологиями, умение коммуницировать в новом формате и быть этичным и внимательным друг к другу» [4] делается на человеческих отношениях, сетевой этике и правилах коммуникации – частично перенесённых из реальной жизни, а частично рождённых виртуальным общением [5]. Важно отметить, что данное понятие носит дискуссионный характер и находится в постоянном эволюционировании, поэтому встречаются разнообразные трактовки [6].

В 2014–2015 годах в рамках проекта «Индекс цифровой грамотности» разработали модель, опирающуюся на многолетний международный опыт медиаобразования, компьютерной и информационной грамотности. Она вклю-

чает четыре компонента:

- технико-технологические возможности с утилитарным уклоном, помогающие осваивать цифровую среду, расширять коммуникации и реализовывать креативный потенциал;

- содержательно-коммуникативные возможности, затрагивающие социокультурные аспекты медиатизированной связи на личном, групповом и массовом уровнях, включая создание и интерпретацию медиатекстов;

- технико-технологические угрозы, связанные с безопасностью устройств и ПО;

- социопсихологические угрозы – наиболее сложная часть, где фокус сосредотачивается на психозетических и этических аспектах [7] (рис. 1).

Сегодня термин «информационная война» звучит чаще, чем когда-либо: в

эпоху постоянных попыток влиять на общественное мнение это один из самых мощных инструментов манипуляции. Под ней понимают целенаправленное воздействие на гражданское население или военных другой страны через распространение ложной целевой информации [8]. В цифровую эпоху фальсифицированные новости и дезинформация стали мощными инструментами воздействия на общественное мнение и формирование массового сознания. Создание и распространение ложных новостей представляют собой тщательно спланированные нарративы, лишённые фактической поддержки, но рассчитанные на влияние на эмоциональное восприятие людей [9]. Методы создания подделанных новостей могут включать в себя различные техники: от искажения фактов до прямого выдумывания событий [10].



**Рисунок 1. Четырёхкомпонентная модель цифровой грамотности [7]**  
**Figure 1. Four-pronged model of digital literacy [7]**

Социальные сети сильно влияют на мировоззрение пользователей. Алгоритмы подбора контента формируют «эхо-камеры», где люди видят лишь подтверждающие их взгляды материалы, усиливая предвзятость и поляризацию общества. Это затрудняет конструктивный диалог [11]. В контексте информационной войны эмоционально заряженная информация усиливает воздействие на коллективное мнение. Эмоции (страх, ненависть) часто перевешивают рациональность, манипулируя поведением масс и общественными процессами [12]. В политике такая манипуляция меняет общественные настроения, отношение к идеям или кандидатам, напрямую влияя на исход выборов. Кроме того, она трансформирует как коллективное, так и индивидуальное поведение: через СМИ и соцсети провоцирует панику, корректирует реакции на события и формирует

восприятие вопросов безопасности [13].

Когнитивные искажения (КИ), будучи естественными продуктами работы нашего мышления, серьёзно осложняют процесс принятия обдуманных и рациональных решений [16, с. 765-768]. Они выступают в роли своеобразных «слепых зон» сознания: сужают восприятие новой или противоречащей информации, искажают воспоминания, формируя фрагментарную картину прошлого, и обостряют тревогу, заставляя концентрироваться на негативе. Эти искажения также негативно влияют на общение, поощряя поспешные суждения, и подрывают критическое мышление. В итоге они становятся питательной средой для устойчивых заблуждений и дезинформации. Американский психолог Дж. Гринспун метко называет КИ «внутренними ментальными фильтрами, которые усиливают страдания, питают тревогу и

заставляют нас чувствовать себя плохо» [15]. Их корни лежат в стремлении мозга экономить энергию: сталкиваясь с огромными потоками данных, он использует ментальные «ярлыки» (эвристики). Хотя такие упрощения иногда эффективны, неудачные «фильтры» чаще приносят вред, чем пользу [16, с. 764].

Цифровая среда может усиливать эти иррациональные паттерны. Как показал онлайн-эксперимент российских психологов И. Попова и А. Вихмана, цифровая грамотность напрямую влияет на адекватность оценки криминальных рисков. Участники, оценивая вероятность преступного поведения по описаниям людей, часто игнорировали реальную статистику, полагаясь на стереотипы и личные предубеждения [17, с. 7]. В условиях, когда информация о преступлениях молниеносно распространяется в сети, подобные искажения ведут к ошибочным выводам и дискриминации. Это доказывает, что навыки критического анализа онлайн-контента и понимания статистических данных сегодня жизненно необходимы.

Для противодействия информационным угрозам требуется комплексный подход. Его фундамент – развитие критического мышления и информационной грамотности населения. Важно научиться не просто потреблять информацию, а подвергать её сомнению: проверять источники, отделять факты от мнений и фейков, искать дополнительные доказательства и рассматривать альтернативные точки зрения перед формированием окончательной позиции.

Ключевую роль здесь играет система образования. Внедрение в учебные программы школ и вузов специальных курсов по медиаграмотности и критическому мышлению – насущная потребность. Эту работу должны дополнять общественные просветительские кампании, рассказывающие о методах информационного манипулирования. При столкновении с подозрительной информацией гражданам необходимо выработать привычку верифицировать её через независимые авторитетные источники.

Правовое регулирование и межгосударственное сотрудничество создают каркас для этой работы. Согласованные законы и совместные стратегии устанавливают рамки борьбы с враждебными кампаниями. Особое значение в этом контексте приобретает цифровая грамотность как превентивный инструмент. Распоряжения Правительства РФ, интегрирующие её в образовательный

процесс, направлены на формирование у граждан «иммунитета» к угрозам: навыков распознавания манипуляций, критического анализа и безопасного использования технологий [18, 19]. Таким образом, право не только создаёт барьеры для агрессоров, но и вооружает общество инструментами психологической устойчивости.

Технологии также предлагают свои решения. Внедрение электронных подписей, блокчейна и подобных инструментов позволяет чётко идентифицировать источник информации и проверять её подлинность. Блокчейн, как цепочка неизменяемых и прозрачно связанных блоков данных, способен существенно снизить риски распространения фальсификаций [20], позволяя пользователям отличать официальный контент от непроверенного.

Только совместная реализация этих мер – образовательных, правовых, технологических и просветительских – способна снизить уязвимость общества перед информационными войнами и укрепить его цифровую безопасность.

Заключение.

Таким образом, результаты исследования позволяют сделать ряд ключевых выводов. В условиях современной информационной войны, где главными инструментами становятся дезинформация и манипуляция, именно цифровая грамотность формирует основу защиты. Она выступает как многослойный щит, который укрепляется системным образованием и поддерживающими технологиями.

Цифровая грамотность – это не просто навык, а комплекс компетенций: способность критически оценивать контент, отличать надёжные источники от фейковых, распознавать манипулятивные приёмы и сознательно препятствовать распространению лжи. Эти умения создают не только личную устойчивость пользователя, но и формируют коллективный «информационный иммунитет» общества. Этот иммунитет критически важен в эпоху стремительного развития искусственного интеллекта и алгоритмических платформ, которые многократно усиливают масштабы и скорость распространения угроз.

Инвестиции в развитие этих компетенций напрямую связаны с укреплением цифрового суверенитета и общей устойчивости социума. Они приводят к конкретным позитивным последствиям: ослабляется влияние дезинформационных кампаний на общественное мнение,

растёт доверие к институтам благодаря развитой способности граждан к верификации информации, и активизируется международное сотрудничество по выработке общих стандартов медиаграмотности.

Следовательно, стратегическая защита лежит в плоскости просвещения, где образование и технологии объединяются для формирования умного и устойчивого общества. Такое общество способно

не только противостоять информационным атакам, но и сохранять интеллектуальную самостоятельность, эффективно используя возможности цифровой эпохи. В итоге это создаёт основу для гармоничного сосуществования человека и технологий. Поэтому инвестиции в цифровую грамотность – это не только мера безопасности, но и необходимый вклад в устойчивое развитие в глобализированном цифровом мире.

### Список источников

1. Gilster P. Digital literacy. New York : John Wiley & Sons, 1997. 279 p. ISBN 978-0-471-07359-3
2. Черноусов И. Цифровая грамотность – must-have среди навыков // Российская газета. 2020. URL: [https://rg.ru/2020/06/08/rabotnikam-na-udalenne-ne-hvataet-cifrovoj-gramotnosti.html].
3. Давыдов С. Г., Логунова О. С. Проект «Индекс цифровой грамотности»: методические эксперименты // Социология: методология, методы, математическое моделирование (4М). 2015. № 41. С. 120–141.
4. Цифровая грамотность россиян: исследования 2020. URL: [https://nafi.ru/analytics/tsifrovaya-gramotnost-rossiyan-issledovanie-2020/].
5. Токтарова В. И., Ребко О. В. Цифровая грамотность: понятие, компоненты и оценка // Вестник Марийского государственного университета. 2021. Т. 15. № 2. С. 165–177.
6. Крумина К. В., Моисеева Н. А. Цифровая грамотность : учебное пособие : в 2 частях. Омск : ОмГТУ, 2023. Часть 1: Основы цифровой грамотности и кибербезопасности. 100 с. ISBN 978-5-8149-3702-5.
7. Шариков А. В. Концепции цифровой грамотности: российский опыт // Коммуникации. Медиа. Дизайн. 2018. Т. 3. № 3. С. 96–112.
8. Аскерова Л. Ф. Информационная война как вид манипуляции // Гуманитарные научные исследования. 2017. № 6. URL: [https://human.snauka.ru/2017/06/24211].
9. Pariser E. The filter bubble: what the Internet is hiding from you. New York : Penguin Group, 2011. 257 p. ISBN 978-0-14-312123-4.
10. Aleinikov A. V., Miletskiy V. P., Strebkov A. I., Pimenov N. P. The «fake-news» phenomenon and transformation of information strategies in the digital society // Scientific and Technical Information Processing. 2019. Т. 46. № 2. С. 117–123.
11. Пономарев Н. Ф. Фейковые новости в контексте постправды // E-SCIO. 2019. № 6 (33). URL: [https://cyberleninka.ru/article/n/feykovyye-novosti-v-kontekste-postpravdy].
12. Хазагеров Г. Г., Лобас П. П. Культурная утилизация манипулятивных технологий // Известия Южного федерального университета. Филологические науки. 2014. № 1. С. 44–52.
13. Демченко А. А., Алиева С. А. Массовое сознание как объект манипуляции в условиях информационной войны // Молодой ученый. 2023. № 51 (498). С. 492–493. URL: [https://moluch.ru/archive/498/109501/].
14. Nikolopoulou K. What is Cognitive Bias? Definition, Types & Examples // Scribbr. 2023. URL: [https://www.scribbr.com/research-bias/cognitive-bias].
15. Grinspoon P. How to Recognize and Tame Your Cognitive Distortions // Harvard Health Publishing. 2022. URL: [https://www.health.harvard.edu/blog/how-to-recognize-and-tame-your-cognitive-distortions-202205042738].
16. Якоба И. А. Когнитивные искажения как средство манипуляции в новостном дискурсе в сфере информационных технологий // Известия Байкальского государственного университета. 2023. Т. 33. № 4. С. 762–771.
17. Попов А. Ю., Вихман А. А. Когнитивные искажения в процессе принятия решений: научная проблема и гуманитарная технология // Вестник ЮУрГУ. Серия «Психология». 2014. Т. 7. № 1. С. 5–15.
18. Об утверждении Концепции информационной безопасности детей в Российской Федерации : распоряжение Правительства Российской Федерации от 28 апр. 2023 г. № 1105-р. URL: [http://publication.pravo.gov.ru/document/0001202304280009].
19. Об утверждении Целевой модели цифровой образовательной среды : приказ Министерства просвещения Российской Федерации от 2 дек. 2019 г. № 649. URL: [http://publication.pravo.gov.ru/document/0001201912020009].
20. Иванов И. И., Петров П. П., Сидоров С. С. Методические материалы по основам информационной безопасности и формированию списка литературы по ГОСТ Р 7.0.5-2008 : пособие для студентов. Москва : ООО «ИнформБезопасность», 2024. 24 с.

### References

1. Gilster, P. (1997). \*Digital literacy\*. New York: John Wiley & Sons, 279 p. ISBN 978-0-471-07359-3.
2. Chernousov, I. (2020). Digital literacy is a must-have skill. \*Rossiyskaya gazeta\*. Available at: [https://rg.ru/2020/06/08/rabotnikam-na-udalenne-ne-hvataet-cifrovoj-gramotnosti.html] (In Russ.).
3. Davydov, S.G., Logunova, O.S. (2015). Project “Digital Literacy Index”: methodological experiments. \*Sotsiologiya: metodologiya, metody, matematicheskoe modelirovanie (4M)\*, 41, 120–141. (In Russ.).
4. Digital literacy of Russians: research 2020. Available at: [https://nafi.ru/analytics/tsifrovaya-gramotnost-rossiyan-issledovanie-2020/] (In Russ.).
5. Toktarova, V.I., Rebko, O.V. (2021). Digital literacy: concept, components and assessment. \*Vestnik Mariyskogo gosudarstvennogo universiteta\*, 15(2), 165–177. (In Russ.).
6. Krumina, K.V., Moiseeva, N.A. (2023). \*Digital literacy: textbook in 2 parts. Part 1: Basics of digital literacy and cybersecurity\*. Omsk: OmGTU, 100 p. ISBN 978-5-8149-3702-5. (In Russ.).

7. Sharikov, A.V. (2018). Concepts of digital literacy: Russian experience. \*Kommunikatsii. Media. Dizayn\*, 3(3), 96–112. (In Russ.).
8. Askerova, L.F. (2017). Information war as a type of manipulation. \*Gumanitarnye nauchnye issledovaniya\*, 6. Available at: [<https://human.snauka.ru/2017/06/24211>] (In Russ.).
9. Pariser, E. (2011). \*The filter bubble: What the Internet is hiding from you\*. New York: Penguin Group, 257 p. ISBN 978-0-14-312123-4.
10. Aleinikov, A.V., Miletskiy, V.P., Strebkov, A.I., Pimenov, N.P. (2019). The “fake-news” phenomenon and transformation of information strategies in the digital society. \*Scientific and Technical Information Processing\*, 46(2), 117–123.
11. Ponomarev, N.F. (2019). Fake news in the context of post-truth. \*E-SCIO\*, 6(33). Available at: [<https://cyberleninka.ru/article/n/feykovye-novosti-v-kontekste-postpravdy>] (In Russ.).
12. Khazagerov, G.G., Lobas, P.P. (2014). Cultural utilization of manipulative technologies. \*Izvestiya Yuzhnogo federalnogo universiteta. Filologicheskie nauki\*, 1, 44–52. (In Russ.).
13. Demchenko, A.A., Alieva, S.A. (2023). Mass consciousness as an object of manipulation in the conditions of information war. \*Molodoy uchenyy\*, 51(498), 492–493. Available at: [<https://moluch.ru/archive/498/109501/>] (In Russ.).
14. Nikolopoulou, K. (2023). What is cognitive bias? Definition, types & examples. \*Scribbr\*. Available at: [<https://www.scribbr.com/research-bias/cognitive-bias/>].
15. Grinspoon, P. (2022). How to recognize and tame your cognitive distortions. \*Harvard Health Publishing\*. Available at: [<https://www.health.harvard.edu/blog/how-to-recognize-and-tame-your-cognitive-distortions-202205042738>].
16. Yakoba, I.A. (2023). Cognitive biases as a means of manipulation in news discourse in the field of information technology. \*Proceedings of the Baikal State University\*, 33(4), 762–771. (In Russ.).
17. Popov, A.Yu., Vikhman, A.A. (2014). Cognitive biases in decision-making: scientific problem and humanitarian technology. \*Vestnik YuUrGU. Seriya “Psikhologiya”\*, 7(1), 5–15. (In Russ.).
18. Government of the Russian Federation (2023). Decree No. 1105-r of April 28, 2023 “On approval of the Concept of information security for children in the Russian Federation”. Available at: [<http://publication.pravo.gov.ru/document/0001202304280009>] (In Russ.).
19. Ministry of Education of the Russian Federation (2019). Order No. 649 of December 2, 2019 “On approval of the Target model of digital educational environment”. Available at: [<http://publication.pravo.gov.ru/document/0001201912020009>] (In Russ.).
20. Ivanov, I.I., Petrov, P.P., Sidorov, S.S. (2024). \*Methodological materials on the basics of information security and compilation of bibliography according to GOST R 7.0.5-2008: manual for students\*. Moscow: OOO “InformBezopasnost”, 24 p. (In Russ.).

**Научный руководитель:**  
**Лунина В. Ю., канд. экон. наук, доцент,**  
**доцент кафедры маркетинга и логистики,**  
**Донецкий филиал РАНХиГС**  
**Донецк, Донецкая Народная Республика,**  
**Российская Федерация**

*Автор заявляет об отсутствии конфликта интересов.*  
*The author declares no conflicts of interests.*

Поступила в редакцию (Reserved) 12.01.2026  
 Поступила после рецензирования 05.02.2026  
 Принята к публикации (Accepted) 10.02.2026