ОРИГИНАЛЬНАЯ СТАТЬЯ

DOI: 10.26794/3033-7097-2025-1-4-51-59
УДК 004.738.5:343.62(045)

Безопасность несовершеннолетних пользователей в информационно-коммуникационной среде

С.Д. Семухин[a], В.В. Пахолюк[b], П.Д. Осина[c], Р.А. Кочкаров[d], С.А. Резниченко[e], Э.А. Окунева[f]
[a, e] Национальный исследовательский ядерный университет «МИФИ», Москва, Российская Федерация;
[b, c, d, f] Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация

АННОТАЦИЯ

Данная статья посвящена всестороннему анализу проблемы обеспечения цифровой безопасности несовершеннолетних в условиях стремительного развития информационного общества и цифровых технологий. **Цель исследования** состоит в выявлении нормативных, организационных и технологических механизмов защиты детей от информационных угроз, формирующихся в сети Интернет, включая деструктивный контент, кибербуллинг, вовлечение в противоправную деятельность и манипулятивные алгоритмы социальных сетей. Особое внимание уделено анализу правовых актов, регулирующих данную сферу, а также институциональной роли государственных органов и значимости образовательных инициатив. **Методологическая основа** исследования включает системный и междисциплинарный подходы, позволяющие учитывать юридические, социокультурные, педагогические и технологические аспекты проблемы. В процессе работы использовались методы контент-анализа нормативных документов, сравнительно-правовой анализ, а также обобщение практического опыта и данных социологических исследований. **Ключевые результаты исследования** заключаются в выявлении фрагментарности существующего законодательства и институциональных механизмов в сфере информационной безопасности несовершеннолетних, а также в обосновании необходимости построения комплексной многоуровневой модели защиты. Эта модель предполагает создание специализированного органа контроля, укрепление связей между школой, семьей и ребенком, а также внедрение современных технических решений для фильтрации и контроля цифрового контента. **Выводы исследования** подчеркивают важность комплексного подхода к решению обозначенной проблемы, необходимость скоординированного межведомственного взаимодействия, развития цифровой грамотности всех участников образовательного процесса, а также совершенствования правового регулирования. Представленные в статье рекомендации и инициативы могут быть использованы при формировании государственной политики в сфере цифровой безопасности, разработке образовательных программ и инструментов защиты детей в онлайн-среде.

Ключевые слова: цифровая безопасность; несовершеннолетние; правовое регулирование; информационные угрозы; интернет; фильтрация контента; родительский контроль

Для цитирования: **Семухин С.Д., Пахолюк В.В., Осина П.Д., Кочкаров Р.А., Резниченко С.А., Окунева Э.А. Безопасность несовершеннолетних пользователей в информационно-коммуникационной среде. *Цифровые решения и технологии искусственного интеллекта.* 2025;1(4):51-59. DOI: 10.26794/3033-7097-2025-1-4-51-59**

ORIGINAL PAPER

Safety of Underage Users in the Information and Communication Environment

S.D. Semukhin[a], V.V. Pakholyuk[b], P.D. Osina[c], R.A. Kochkarov[d], S.A. Reznichenko[e], E.A. Okuneva[f]
[a, e] National Research Nuclear University "MEPhI", Moscow, Russian Federation;
[b, c, d, f] Financial University under the Government of the Russian Federation, Moscow, Russian Federation

ABSTRACT

This article presents a comprehensive analysis of the issue of ensuring digital safety for minors in the context of the rapid development of the information society and digital technologies. **The objective of the study** is to identify the legal, organizational, and technological mechanisms for protecting children from informational threats emerging in the online environment, including harmful content, cyberbullying, involvement in illegal activities, and manipulative algorithms of social media platforms. Special attention is given to the analysis of legal regulations governing this area, the institutional role of state authorities, and the importance of educational initiatives. **The methodological basis** of the study includes a systematic and interdisciplinary approach, taking into account the legal, sociocultural, pedagogical, and technological dimensions of the problem. The research employs methods such as content analysis of legal documents, comparative legal analysis, as well as synthesis of practical experience and sociological data. **The key findings** of the study highlight the fragmented nature of current legislation and institutional mechanisms in the field of digital safety for minors. The study substantiates the need for the development of a comprehensive multi-level protection model. This

model includes the establishment of a specialized supervisory body, strengthening cooperation between schools, families, and children, and implementing modern technological tools for filtering and monitoring digital content. **The conclusions** of the article emphasize the importance of an integrated approach to addressing the identified problem, the need for coordinated interagency cooperation, the promotion of digital literacy among all participants in the educational process, and the improvement of legal frameworks. The recommendations and initiatives presented in this study may serve as a foundation for the development of public policy in the area of digital safety, the design of educational programs, and the implementation of child protection tools in the online environment.

Keywords: digital safety; minors; legal regulation; informational threats; Internet; content filtering; parental control

For citation: **Semukhin S.D., Pakholyuk V.V., Osina P.D., Kochkarov R.A., Reznichenko S.A., Okuneva E.A. Safety of underage users in the information and communication environment. *Digital Solutions and Artificial Intelligence Technologies*. 2025;1(4):51-59. DOI: 10.26794/3033-7097-2025-1-4-51-59**

ВВЕДЕНИЕ

Современное общество стремительно развивается в направлении цифровизации всех сфер жизнедеятельности. Особую актуальность в этом контексте приобретает проблема обеспечения информационной безопасности несовершеннолетних. С каждым годом увеличивается вовлеченность детей и подростков в интернет-пространство, что сопровождается ростом рисков, связанных с воздействием вредоносного контента, интернет-мошенничеством, психологическим манипулированием и нарушением их прав на неприкосновенность частной жизни.

Несмотря на то, что цифровые технологии предоставляют широкие возможности для обучения, социализации и саморазвития, они одновременно создают новые угрозы, с которыми несовершеннолетние не всегда в состоянии справиться самостоятельно. Поэтому возникает необходимость в системной защите детей в цифровой среде, включающей как нормативно-правовое регулирование, так и практические механизмы профилактики и вмешательства.

Цель исследования состоит в выявлении нормативных, организационных и технологических механизмов защиты детей от информационных угроз, формирующихся в сети Интернет.

ПРАВОВЫЕ ОСНОВЫ ЗАЩИТЫ НЕСОВЕРШЕННОЛЕТНИХ В ЦИФРОВОЙ СРЕДЕ

Правовая защита несовершеннолетних в цифровой среде в Российской Федерации опирается на комплекс федеральных законов, международных соглашений и подзаконных актов, регулирующих вопросы информационной безопасности, прав ребенка и ограничения доступа к вредоносной информации. Среди ключевых документов можно выделить:

- Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[1];
- Федеральный закон № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»[2];
- Федеральный закон № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»[3];
- Концепция информационной безопасности детей, утвержденная в 2015 году[4];
- Конвенция о правах ребенка (1989), ратифицированная Российской Федерацией[5];
- Приказ Минкомсвязи России № 161 от 16.06.2014[6].

Однако, несмотря на наличие нормативной базы, значительная часть этих документов не содержит четко определенных механизмов привлечения к ответственности лиц, наносящих вред несовершеннолетним в интернете. Это порождает правовые лакуны и затрудняет применение законодательства на практике.

Особую тревогу вызывает активность злоумышленников в социальных сетях, которые с легкостью выходят на контакт с детьми, используя их довер-

[1] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 30.12.2021) «Об информации, информационных технологиях и о защите информации». URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 13.02.2023).

[2] Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 01.07.2021) «О защите детей от информации, причиняющей вред их здоровью и развитию». URL: https://www.consultant.ru/document/cons_doc_LAW_108808/ (дата обращения: 13.02.2023).

[3] Федеральный закон от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации» (последняя редакция). URL: https://www.consultant.ru/document/cons_doc_LAW_19558/ (дата обращения: 13.02.2023).

[4] Концепция информационной безопасности детей (2015 г.). URL: http://static.government.ru/media/files/mPbAMyJ29uSPhL3p20168GA6hv3CtBxD.pdf (дата обращения: 13.02.2023).

[5] Конвенция о правах ребёнка (одобрена Генеральной Ассамблеей ООН 20.11.1989, вступила в силу для СССР 15.09.1990). URL: https://www.consultant.ru/document/cons_doc_LAW_9959/ (дата обращения: 13.02.2023).

[6] Приказ Минкомсвязи России от 16.06.2014 № 161 «Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию». URL: https://digital.gov.ru/ru/documents/4446/ (дата обращения: 13.02.2023).

чивость и недостаток критического мышления, получение личной информации путем обмана, вовлечение в деструктивные сообщества, а также распространение вредоносного контента [1].

Цифровая реклама представляет собой еще один значимый источник информационного давления на несовершеннолетних [2, 3, 4]. Она появляется не только в браузерах, но и во всех цифровых устройствах — смартфонах, планшетах, телевизорах с выходом в интернет. Под видом развлекательного контента рекламодатели продвигают товары и идеи, к которым дети могут оказаться не готовы ни интеллектуально, ни эмоционально (*рис. 1–3*).

На данный момент регулирование рекламного контента в детской цифровой среде остается фрагментарным. Отсутствуют действенные инструменты идентификации и блокировки скрытой рекламы, направленной на манипуляцию детским поведением. В результате несовершеннолетние становятся уязвимой целевой аудиторией, подверженной потребительским и психологическим установкам, формируемым через рекламные алгоритмы.

Защита прав и интересов детей в цифровой среде входит в компетенцию сразу нескольких государственных органов, каждый из которых действует в рамках своей сферы ответственности. Среди них:

- Роскомнадзор, осуществляющий надзор за соблюдением законодательства в сфере связи, информационных технологий и защиты персональных данных.
- Рособрнадзор, контролирующий образовательные учреждения и внедрение цифровых платформ в обучении.
- Роспотребнадзор, отвечающий за защиту прав потребителей, в том числе в цифровой среде.

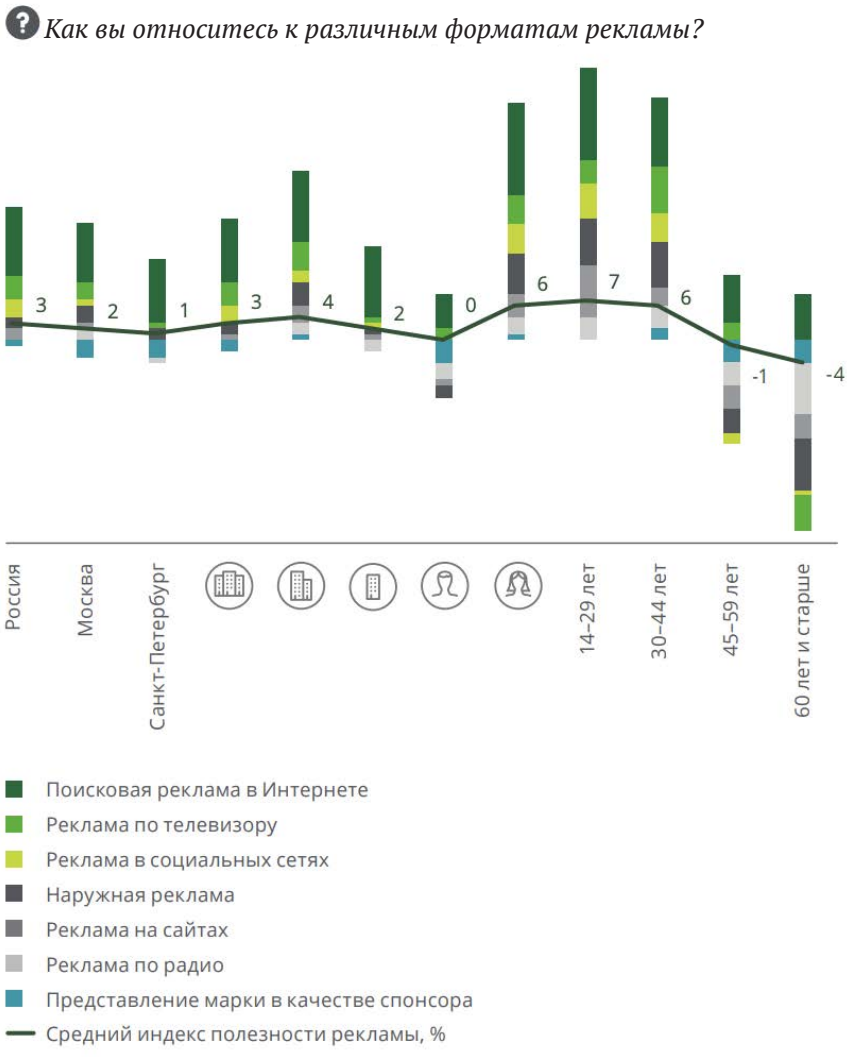

Рис. 1 / Fig. 1. **Лояльность к различным форматам рекламы среди возрастных групп / Loyalty to Different Advertising Formats among Age Groups**

Источник / Source: исследовательский центр компании «Делойт» в СНГ / Deloitte CIS Research Center [3].

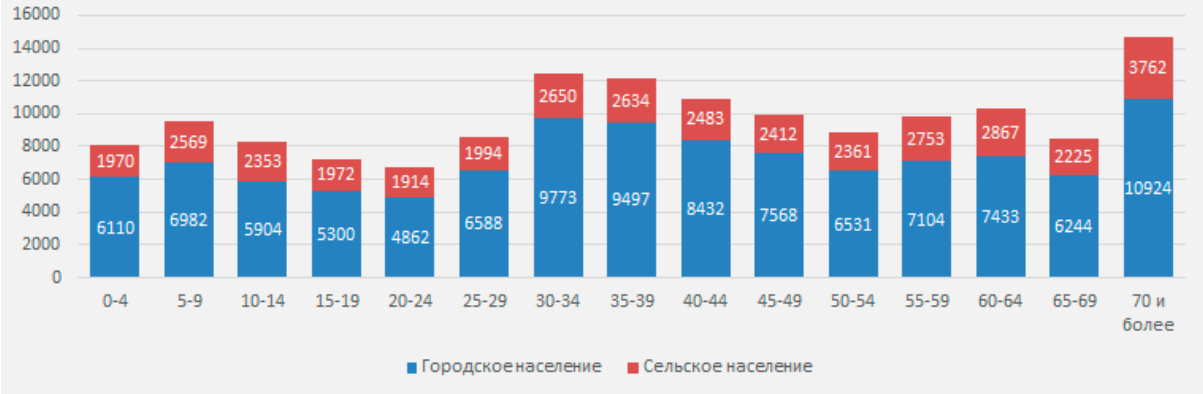

Рис. 2 / Fig. 2. **Демографическое распределение населения России по возрасту (2021) / Demographic Distribution of the Russian Population by Age (2021)**

Источник / Source: Информационно-статистический портал InfoTables / InfoTables. URL: https://infotables.ru/statistika/31-rossijskaya-federatsiya/783-raspredelenie-naseleniya-po-vozrastnym-gruppam-tablitsa

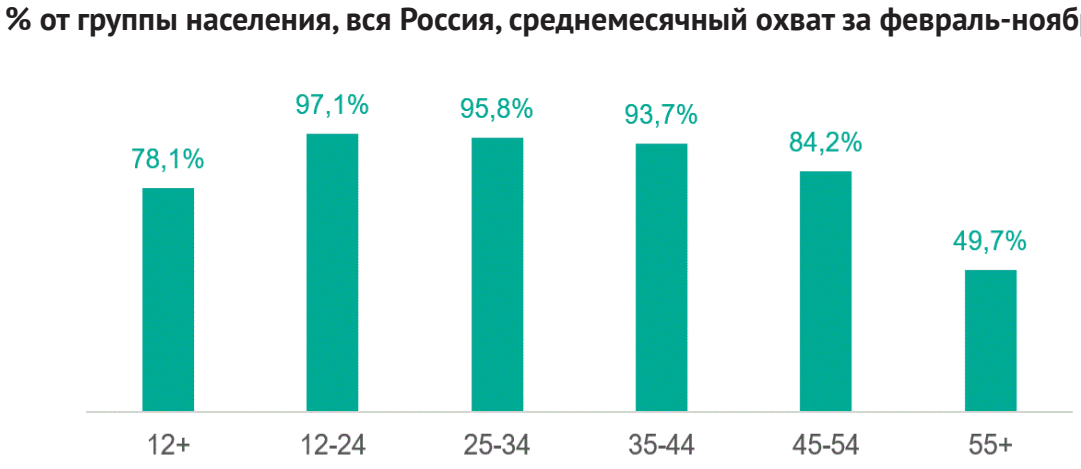

Рис. 3 / Fig. 3. **Возрастная структура аудитории интернета в России / Age Structure of Internet Audience in Russia**

Источник / Source: исследовательская компания Mediascope / Mediascope Research Company [4]

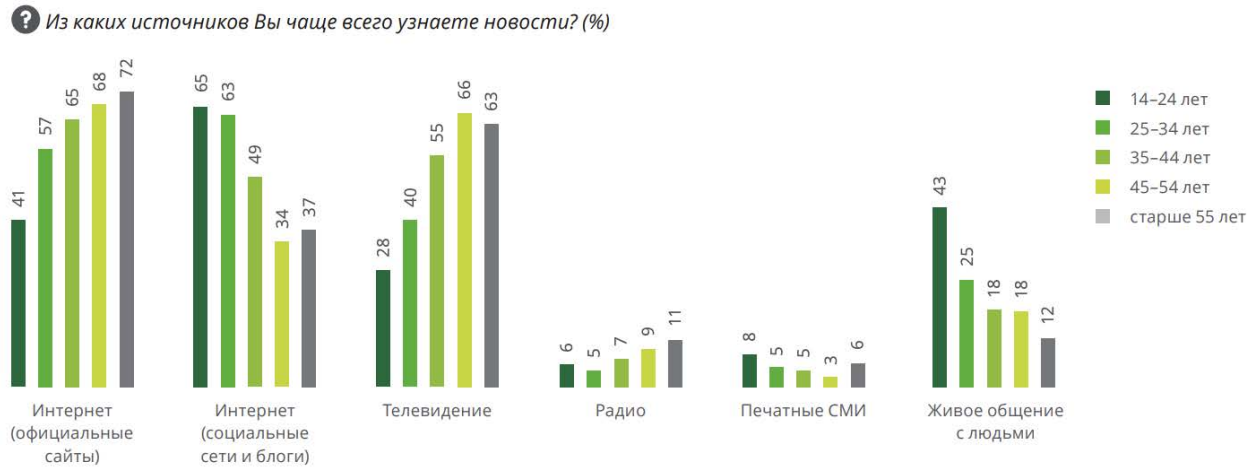

Рис. 4 / Fig. 4. **Использование медиаконтента разными возрастными группами / Use of Media Content by Different Age Groups**

Источник / Source: исследовательский центр компании «Делойт» в СНГ / Deloitte CIS Research Center [3].

• Министерство просвещения, разрабатывающие методические рекомендации и образовательные программы, включая темы цифровой грамотности.

Несмотря на вовлеченность различных ведомств, их усилия не объединены в единую координированную систему. Отсутствие межведомственного взаимодействия приводит к дублированию функций и снижает общую эффективность работы по обеспечению цифровой безопасности детей. Следовательно, необходим комплексный подход, основанный на координации, обмене данными и общей стратегии защиты.

МОДЕЛЬ ЗАЩИТЫ НЕСОВЕРШЕННОЛЕТНИХ В ЦИФРОВОЙ СРЕДЕ

Для преодоления разрозненности и повышения эффективности предлагается внедрение модели многоуровневой защиты несовершеннолетних в цифровой среде. Эта модель включает три ключевых уровня.

1. Формирование связки «родители — школа — ребенок». Цифровая социализация детей невозможна без активного участия взрослых. Родители и педагоги должны обладать знаниями и навыками, необходимыми для сопровождения детей в цифровом пространстве.

2. Технические алгоритмы фильтрации контента. Необходима разработка и внедрение программных решений, которые позволяют ограничивать доступ к вредоносной информации на всех устройствах, используемых несовершеннолетними (*рис. 5*) [5].

Это включает использование интеллектуальных фильтров, систем родительского контроля и сотрудничество с крупными IT-компаниями.

В рамках рассматриваемого проекта авторами были реализованы следующие инициативы, направленные на повышение цифровой безопасности несовершеннолетних:

• разработан обучающий веб-сайт, включающий видеокурсы и инструкции для родителей, касающиеся защиты детей в интернете [6];

• создан Telegram-бот, предоставляющий рекомендации и экстренные меры в случае выявления потенциальной угрозы[7].

Эти инструменты позволяют оперативно реагировать на информационные угрозы, а также обеспечивают доступ к проверенным знаниям о безопасности в сети.

Отдельного внимания заслуживает феномен видеохостинга TikTok и других социальных плат-

[7] Родительский контроль ИБ21–4. URL: https://web.telegram.org/z/#2108045873; Telegram: @TestbotIB 214fu_bot.

Рис. 5 / Fig. 5. **Рекомендуемое потребление цифрового контента по категориям в течение дня (пирамида контента) / Recommended Consumption of Digital Content by Category throughout the Day (Content Pyramid)**

Источник / Source: онлайн-журнал «Лайфхакер» / Lifehacker.ru [5].

форм, чьи алгоритмы персонализированной ленты способны формировать новые установки, вкусы и поведенческие модели. Пользователь сам не замечает, как оказывается в информационном пузыре, где его интересы подкрепляются визуальным контентом, эмоционально окрашенным и зачастую деструктивным [1].

Особенно подвержены подобному воздействию подростки, находящиеся в процессе формирования идентичности. Алгоритмы могут не только подстроиться под интересы пользователя, но и усилить его тревожность, внушить искаженные представления о себе и мире [7]. Это создает угрозу психологическому и ментальному здоровью детей, делая необходимым государственный и общественный контроль над алгоритмическими системами.

Одним из препятствий на пути к эффективной защите детей в цифровой среде является культурный разрыв между поколениями. Родители, выросшие в доцифровую эпоху, зачастую опираются на постфигуративные модели воспитания, которые не учитывают реалии сетевой жизни [8]. Между тем дети проводят в интернете значительную часть времени, формируя там не только круг общения, но и мировоззрение.

Отсутствие понимания между поколениями приводит к тому, что взрослые либо чрезмерно ограничивают доступ к сети, вызывая протест, либо, напротив, полностью игнорируют происходящее. Оба подхода неэффективны и требуют пересмотра в сторону сотрудничества и совместного освоения цифровой среды.

3. Создание специализированного координационного органа по цифровой безопасности детей (например, Федеральной службы по детскому информационному контролю — ФСДИК).

В условиях стремительного развития цифровых технологий и усложнения структуры информационного пространства становится все более очевидной необходимость формирования специализированного государственного органа, деятельность которого будет направлена исключительно на обеспечение цифровой безопасности несовершеннолетних. Предлагаемое учреждение, условно обозначаемое как Федеральная служба по детскому информационному контролю (ФСДИК), должно выполнять не карательную, а превентивную, координационную и образовательную функции. В отличие от уже существующих органов, таких как Роскомнадзор, Роспотребнадзор или Минпросвещения, новый институт должен обладать узкой, но глубокой специализацией, касающейся исключительно защиты детей в цифровой среде.

Основной задачей ФСДИК станет непрерывный мониторинг интернет-пространства с акцентом на выявление потенциально опасных информационных источников, таких как сайты с деструктивным контентом, группы в социальных сетях, распространяющие радикальные или манипулятивные идеи, а также платформы, провоцирующие девиантное поведение у подростков. Особое внимание может уделяться отслеживанию новых форм цифрового насилия, включая кибербуллинг, груминг, шантаж, цифровое преследование и вовлечение несовершеннолетних в противоправные действия.

Второе направление работы предполагает разработку методических материалов и рекомендаций для широкого круга адресатов: родителей, педагогов, администраторов образовательных учреждений, представителей IT-индустрии и контент-платформ. Эти рекомендации должны носить не только информационный, но и прикладной характер, включая чек-листы для оценки цифровой среды, инструкции по настройке фильтров и алгоритмы реагирования на критические ситуации. Такой подход обеспечит доступность и применимость знаний на практике [9].

ФСДИК также может выполнять аналитическую функцию, формируя предложения по совершенствованию действующего законодательства. Учитывая динамичность цифровой среды, необходимо регулярно адаптировать правовые нормы, выявлять пробелы в законодательстве и разрабатывать новые регулятивные механизмы. В этом контексте служба может стать связующим звеном между экспертным сообществом, законодателями и органами исполнительной власти.

Не менее важной задачей нового органа станет реализация масштабных просветительских и обучающих программ. Подобные кампании могут включать национальные информационные недели, цифровые марафоны, выпуск видеоконтента и проведение онлайн-курсов, ориентированных на родителей, школьников и учителей [10]. Это позволит не только повысить общий уровень цифровой грамотности, но и сформировать у подрастающего поколения навыки критического мышления, саморегуляции и ответственного поведения в сети.

Наконец, при разработке концепции и структуры ФСДИК важно учесть вопросы этики, соблюдения прав ребенка, неприкосновенности личной жизни и соразмерности вмешательства. Орган должен действовать в логике партнерства с гражданским обществом, ИТ-компаниями и международ-

ными организациями, обеспечивая прозрачность своих действий и открытость к диалогу. В этом случае он сможет не только оперативно реагировать на цифровые угрозы, но и стать основой устойчивой и гуманной системы защиты детей в быстро меняющемся информационном мире.

ВЫВОДЫ

Таким образом, проблема информационной безопасности несовершеннолетних в цифровом пространстве является многогранной и требует междисциплинарного подхода. Необходимо не только совершенствовать законодательную базу и вводить технические ограничения, но и формировать культуру цифровой грамотности среди всех участников образовательного и семейного процесса.

Создание комплексной системы защиты с четким распределением ответственности между государством, обществом и семьей позволит обеспечить условия для безопасного, развивающего и гуманного информационного пространства, в котором подрастающее поколение сможет реализовывать свои возможности без угрозы своему благополучию.

СПИСОК ИСТОЧНИКОВ

1. Фефелов А., Афанасьев А. Дети Интернета: что они смотрят и кто ими управляет. М.: Изд-во «Наше завтра»; 2021. 314 с. URL: https://djvu.online/file/CJ7HiFQB4Ysxx?ysclid=mj6l7w5e2v860671556
2. Полякова Т.А. Цифровизация и синергия правового обеспечения информационной безопасности. *Информационное право*. 2019;2(60):4–7. URL: https://elibrary.ru/item.asp?id=39173932
3. Табакова О., Шульга А., Родионова В. и др. Медиапотребление в России – 2021. Исследовательский центр компании «Делойт» в СНГ. URL: https://nlr.ru/reader/dep/artupload/reader/article/RA6550/NA65935.pdf
4. Пикулева М. Аудитория Интернета в России в 2020 году. Mediascope. URL: https://mediascope.net/news/1250827/
5. Евстафьева Е. Как сесть на здоровую информационную диету. Лайфхакер. 28.07.2018. URL: https://lifehacker.ru/informacionnaya-dieta/
6. Лазарев Д., Семухин С., Амитин М., Левченко Д. Родительский контроль. URL: https://festive-stonebraker-ecb381.netlify.app/
7. Мамаева А.Е. Меры предупреждения вовлечения несовершеннолетних посредством сети Интернет. Проблемы квалификации ст. 150 УК РФ. *Вопросы российского и международного права*. 2022;12(2А):236–242. DOI: 10.34670/AR.2022.12.36.027
8. Андреева Д.А. Проблема детско-родительских отношений в транзитивном обществе. *Психологическая наука и образование*. 2016;7(31):12–20. URL: https://www.elibrary.ru/whycyz
9. Степанова Н.А. Обеспечение информационной безопасности детей в цифровом пространстве. *Гуманитарные исследования Центральной России*. 2024;1(30):60-77. DOI: 10.24412/2541-9056-2024-130-59-77
10. Боровских В.А., Петрова С.С. Формирование безопасного поведения в интернете у младших школьников. *Мир педагогики и психологии*: международный научно-практический журнал. 2023;04(81). URL: https://scipress.ru/pedagogy/articles/formirovanie-bezopasnogo-povedeniya-v-internete-u-mladshikh-shkolnikov.html

REFERENCES

1. Fefelov A., Afanasiev A. Children of the Internet: What They Watch and Who Controls Them. Moscow: Publishing House “Nashe vremia”; 2021. 314 p. URL: https://djvu.online/file/CJ7HiFQB4Ysxx?ysclid=mj6l7w5e2v860671556 (In Russ.).
2. Polyakova T.A. Digitalization and Synergy of Legal Support for Information Security. *Information Law*. 2019;2(60):4-7. URL: https://elibrary.ru/item.asp?id=39173932 (In Russ.).
3. Tabakova O., Shulga A., Rodionova V. et al. Media consumption in Russia – 2021. Research Center of Deloitte CIS. URL: https://nlr.ru/reader/dep/artupload/reader/article/RA6550/NA65935.pdf (In Russ.).
4. Pikuleva M. Internet Audience in Russia in 2020. Mediascope. URL: https://mediascope.net/news/1250827/ (In Russ.).
5. Evstafieva E. How to Start a Healthy Information Diet. Livehacker. 28.07.2018. URL: https://lifehacker.ru/informacionnaya-dieta/ (In Russ.).
6. Lazarev D., Semukhin S., Amitin M., Levchenko D. Parental control. URL: https://festive-stonebraker-ecb381.netlify.app/ (In Russ.).

7. Mamaeva A.E. Measures to prevent the involvement of minors through the Internet. Problems of qualification Art. 150 of the Criminal Code of the Russian Federation. *Voprosy rossiiskogo i mezhdunarodnogo prava*. 2022;12(2A):236–242. (In Russ.). DOI: 10.34670/AR.2022.12.36.027
8. Andreeva D.A. The Problem of Parent-Child Relationships in a Transitive Society. *Psychological Science and Education*. 2016;7(31):12-20. URL: https://www.elibrary.ru/whycyz (In Russ.).
9. Stepanova N.A. Ensuring the information security of children in the digital space. *Humanities researches of the Central Russia*. 2024;1(30):60-77. (In Russ.). DOI: 10.24412/2541-9056-2024-130-59-77
10. Borovskikh V.A., Petrova S.S. Formation of safe behavior on the Internet among younger schoolchildren. *Mir pedagogiki i psikhologii*: International Scientific Journal. 2023;04(81). URL: https://scipress.ru/pedagogy/articles/formirovanie-bezopasnogo-povedeniya-v-internete-u-mladshikh-shkolnikov.html (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ / ABOUT THE AUTHORS

Сергей Дмитриевич Семухин — студент программы магистратуры, Национальный исследовательский ядерный университет «МИФИ», Москва, Российская Федерация
Sergey D. Semukhin — Master Programme Student, National Research Nuclear University "MEPhI", Moscow, Russian Federation
https://orcid.org/0000-0002-2622-5879
semukhin.serezha@mail.ru

Владимир Всеволодович Пахолюк — студент программы бакалавриата факультета информационных технологий и анализа больших данных, Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация
Vladimir V. Pakholiuk — Bachelor Programme Student, Faculty of Information Technology and Big Data Analysis, Financial University under the Government of the Russian Federation, Moscow, Russian Federation
https://orcid.org/0009-0002-2758-1127
237521@edu.fa.ru

Полина Дмитриевна Осина — студентка программы бакалавриата факультета информационных технологий и анализа больших данных, Финансовый университета при Правительстве Российской Федерации, Москва, Российская Федерация
Polina D. Osina — Bachelor Programme Student, Faculty of Information Technology and Big Data Analysis, Financial University under the Government of the Russian Federation, Moscow, Russian Federation
https://orcid.org/0009-0000-8187-0937
polina.osina005@gmail.com

Расул Ахматович Кочкаров — кандидат экономических наук, доцент кафедры искусственного интеллекта факультета информационных технологий и анализа больших данных, Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация
Rasul A. Kochkarov — Cand. Sci. (Econ.), Associate Professor of the Department of Artificial Intelligence, Faculty of Information Technology and Big Data Analysis, Financial University under the Government of the Russian Federation, Moscow, Russian Federation
https://orcid.org/0000-0003-3186-3901
rkochkarov@fa.ru

Сергей Анатольевич Резниченко — кандидат технических наук, доцент, доцент кафедры стратегии и технологии кибербезопасности Института интеллектуальных кибернетических систем, Национальный исследовательский ядерный университет «МИФИ», Москва, Российская Федерация
Sergey A. Reznichenko — Cand. Sci. (Tech.), Assoc. Prof., Assoc. Prof. of Cybersecurity Strategy and Technologies Department of the Institute of Intelligent Cybernetic Systems, National Research Nuclear University "MEPhI", Moscow, Russian Federation
https://orcid.org/0000-0002-1539-0457
rsa_5@bk.ru

Эвелина Александровна Окунева — ассистент кафедры математики и анализа данных факультета информационных технологий и анализа больших данных, Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация
Evelina A. Okuneva — Assistant of the Department of Mathematics and Data Analysis, Faculty of Information Technology and Big Data Analysis, Financial University under the Government of the Russian Federation, Moscow, Russian Federation
https://orcid.org/0009-0006-4385-4462
Автор для корреспонденции / Corresponding author:
eaokuneva@fa.ru

Заявленный вклад авторов:
С.Д. Семухин — концепция исследования, обзор литературы, написание первоначального варианта текста (введение, часть аналитического раздела).
В.В. Пахолюк — сбор и анализ статистических данных, разработка и описание технических инструментов (веб-сайт, Telegram-бот).
П.Д. Осина — анализ нормативно-правовой базы, сравнительно-правовой анализ, работа над разделом о государственном регулировании.
Р.А. Кочкаров — научное руководство, методология исследования, критический анализ и доработка текста, формулировка выводов.
С.А. Резниченко — координация работы над статьей, консультирование по технологическим аспектам безопасности, анализ алгоритмов фильтрации контента, рецензирование.
Э.А. Окунева — финальное редактирование и оформление, подготовка аннотаций и ключевых слов, список литературы.

Authors' declared contributions:
S.D. Semukhin — research concept, literature review, drafting the initial version of the text (Introduction, part of the analytical section).
V.V. Pakholyuk — collection and analysis of statistical data, development and description of technical tools (website, Telegram bot).
P.D. Osina — analysis of the legal and regulatory framework, comparative legal analysis, work on the section concerning state regulation.
R.A. Kochkarov — scientific supervision, research methodology, critical analysis and revision of the text, formulation of conclusions.
S.A. Reznichenko — coordination of work on the article, consulting on technological aspects of security, analysis of content filtering algorithms, reviewing.
E.A. Okuneva — final editing and formatting, preparation of abstracts and keywords, reference list.

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.
Conflicts of Interest Statement: The authors have no conflicts of interest to declare.

Статья поступила в редакцию 13.10.2025; принята к публикации 24.11.2025.
Авторы прочитали и одобрили окончательный вариант рукописи.
The article was submitted on 13.10.2025; accepted for publication on 24.11.2025.
The authors read and approved the final version of the manuscript.