Плетнёв Дмитрий Сергеевич
бакалавр, преподаватель
Красноярский филиал ФГОБУ ВО «Финансовый университет
при Правительстве Российской Федерации»
г. Красноярск, Красноярский край

ЗАЩИТА НЕСОВЕРШЕННОЛЕТНИХ В ЦИФРОВОМ ПРОСТРАНСТВЕ: ПРАВОВЫЕ МЕХАНИЗМЫ И ПРЕВЕНТИВНЫЕ МЕРЫ

Аннотация: *цифровое пространство сегодня – неотъемлемая часть жизни любого человека, но наибольшую активность в интернете проявляют дети. Согласно статистике, подростки в возрасте 12–17 лет пользуются интернетом ежедневно, проводя в среднем более 6 часов в сутки онлайн. Социальные сети, мессенджеры, развлекательные приложения – всё это может стать платформами, несущими потенциальную опасность для детей: утечка персональных данных, вредоносный контент, кибербуллинг, вовлечение в преступные сообщества.*

В связи с этим защита несовершеннолетних в цифровом пространстве – задача, которая требует комплексного подхода: взаимодействия государства, образовательных учреждений, родителей и детей.

В статье представлены правовые механизмы, регулирующие использование интернета детьми, и превентивные меры, обеспечивающие безопасность несовершеннолетних в сети.

Ключевые слова: *цифровое пространство, кибербуллинг, троллинг, кибербезопасность, цифровая гигиена, онлайн-груминг, цифровая зависимость.*

Процесс цифровой трансформации социума открывает множество новых возможностей для самореализации и развития молодого поколения, вместе с тем ставя под серьёзную угрозу их безопасность в сети. Согласно исследованиям, проведенным онлайн-школой «Фоксфорд», больше половины опрошенных подростков (55%) сталкивались с кибербуллингом. В большинстве случаев

юные респонденты имели дело с троллингом (грубость, оскорбления в свой адрес) – 84% опрошенных [7].

Одним из первых документов, определивших общие принципы защиты детей от вредной информации, которые в дальнейшем развивались в контексте цифрового пространства, стала Конвенции ООН о правах ребенка 1989 года.

Статья 17 обязывает государства-участники «признавать важную роль средств массовой информации и обеспечивать, чтобы ребёнок имел доступ к информации и материалам из различных национальных и международных источников, особенно к таким информации и материалам, которые направлены на содействие социальному, духовному и моральному благополучию, а также здоровому физическому и психическому развитию ребёнка» [3].

Пункт «е» этой статьи предписывает государствам «поощрять разработку надлежащих принципов защиты ребёнка от информации и материалов, наносящих вред его благополучию, учитывая положения статей 13 и 18» [3].

Главным нормативным актом, обеспечивающим безопасность детей от вредной информации в Российской Федерации, является Федеральный закон №436-ФЗ от 29 декабря 2010 года «О защите детей от информации, причиняющей вред их здоровью и развитию». Документ определяет пять ступеней возрастной классификации контента (0+, 6+, 12+, 16+, 18+) и обязывает распространителей информации указывать возрастные ограничения. С 2021 года закон также регулирует распространение информации в социальных сетях и мессенджерах [9].

Защиту персональных данных несовершеннолетних определяет Федеральный закон №152-ФЗ «О персональных данных», содержащий специальные положения о защите персональных данных детей. Например, законом запрещена обработка биометрических данных несовершеннолетних без согласия родителей [10].

Административная ответственность за распространение среди детей продукции, «содержащей информацию, причиняющую вред их здоровью или развитию, если это действие не содержит уголовно наказуемого деяния», преду-

смотрена статьей 6.17 Кодекса Российской Федерации об административных правонарушениях (КоАП РФ) [2].

Уголовная ответственность наступает по следующим статьям [8].

1. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (ст. 242.1 УК РФ).

2. Вовлечение несовершеннолетних в противоправную деятельность (ст. 150 УК РФ).

3. Сексуальная эксплуатация детей в интернете (ст. 135 УК РФ).

Несмотря на наличие нормативно-правовых актов, на сегодняшний день можно обозначить следующие проблемы.

1. Возрастная маркировка не соответствует содержанию контента.

2. Глобальный характер интернета создаёт трудности в реализации российского законодательства в отношении иностранных ресурсов.

3. Стремительное развитие технологий опережает правовое регулирование.

К основным превентивным мерам обеспечения цифровой безопасности можно отнести следующие: технические средства защиты, цифровая гигиена и просветительские программы, профилактика специфических угроз.

Технические средства защиты. Одним из инструментов, ограничивающих доступ несовершеннолетних к запрещенным материалам, является система родительского контроля, работающая как на уровне операционных систем (Google Family Link, Apple Screen Time), так и посредством провайдера интернет-услуг и оператора сотовой связи.

Родительский контроль позволяет фильтровать контент по заданным словам и категориям, устанавливать ограничение на пребывание в сети, блокировать доступ к опасным приложениям и сайтам, отслеживать местонахождение ребёнка.

Следует отметить и развитие технологий возрастной верификации в цифровом пространстве. В Общественной палате предложили ввести идентификацию для доступа к контенту 18+ в интернете. Евгений Машаров, член Научно-консультативного совета при Общественной палате Российской Федерации,

утверждает: «Развитие технологий нельзя останавливать, однако меры по защите детей и обеспечению безопасного цифрового пространства необходимо принимать уже сегодня. Отдельные несовершеннолетние под влиянием интернет-среды попадают в рискованные ситуации, в том числе вовлекаются в противоправные действия ради небольшого вознаграждения» [6].

Понятие «цифровая гигиена» было впервые опубликовано в 2006 году специалистом по кибербезопасности Эдуардо Гельбштайном в книге «Good Digital Hygiene: A guide to staying secure in cyberspace».

Цифровая гигиена – это «совокупность практик, правил и организационных мероприятий, направленных на безопасное, ответственное и здоровое использование цифровых устройств, сервисов и сетевых ресурсов» [1].

Цифровую гигиену необходимо рассматривать как неотъемлемую составляющую воспитания современного подростка. Основные принципы:

– обучение критическому восприятию информации;

– работа по защите персональных данных;

– формирование навыков уважительного общения в онлайн-коммуникации;

– установление «цифровых границ» в семье (например, отказ от использования гаджета во время приёма пищи).

В рамках просветительской деятельности Министерство просвещения РФ разработало методические рекомендации по реализации мер информационной безопасности детей в образовательных организациях, которые предполагают внедрение тем цифровой безопасности в учебные программы и проведение периодических родительских собраний по данной тематике [5].

Противодействие специфическим угрозам.

Эффективная профилактика кибербуллинга предполагает:

– открытие анонимных каналов информирования о травле в школе;

– разработку курсов повышения квалификации для педагогов по распознаванию признаков кибербуллинга;

– создание психологической службы для профилактической работы с потенциальными жертвами и агрессорами.

Особого внимания требует онлайн-груминг – «сексуальное домогательство по отношению к детям, реализуемого в сети интернет, и разновидности сексуальной эксплуатации детей» [4].

Профилактическая работа подразумевает обучение детей распознавать манипуляцию (чрезмерную заинтересованность незнакомца, просьбы оставить в секрете общение, предложения встреч и пр.) и незамедлительно ставить в известность родителей или учителей о подозрительных контактах.

Еще одна потенциальная опасность – «цифровое слабоумие». Манфред Шпитцер, немецкий нейробиолог и психиатр, определяет его как «чрезмерное использование цифровых устройств, приводящее к разрушению познавательных способностей» [11].

Основные идеи Шпитцера:

– чрезмерное использование гаджетов приводит к социальной изоляции; снижает эмпатию; провоцирует проблемы с эмоциональной регуляцией; формирует «клиповое мышление»;

– раннее приобщение детей к виртуальному миру «отрывает» их от реальной жизни, что имеет негативные последствия для когнитивных процессов.

Рекомендации, предложенные М. Шпитцером в контексте проблемы цифровой зависимости: ограничение пребывания детей в интернете, исключение гаджетов из процесса обучения, тренировка памяти и внимания посредством заучивания материала, развивающих игр, анализа и пересказа текстов, стимулирование офлайн-активности (живое общение с семьей, друзьями, чтение книг, прогулки на свежем воздухе, занятие спортом), что стимулирует работу различных участков мозга.

Для обеспечения безопасности детей в цифровом пространстве необходим комплексный подход, сочетающий строгое правовое регулирование, применение современных технических решений и полноценная просветительская деятельность. Только при системной работе по формированию у детей навыков цифровой гигиены и создании безопасной инфраструктуры возможна реализация их прав в цифровую эпоху без ущерба для здоровья и самореализации.

Список литературы

1. Гельбштейн Э. Good Digital Hygiene: A guide to staying secure in cyberspace / Э. Гельбштейн. – 1-е изд. – Bookboon.com, 2013. – 86 с. – ISBN 978-87-403-0577-7.

2. Кодекс об административных правонарушениях (КоАП РФ). – URL: https://base.garant.ru/12125267/ (дата обращения: 16.02.2026).

3. Конвенция о правах ребёнка (Нью-Йорк, 20 ноября 1989 г.) // Ведомости Съезда народных депутатов СССР и Верховного Совета СССР. – 1990. – №45. – Ст. 955.

4. Медведева А.С. Характеристики онлайн груминга как вида сексуальной эксплуатации несовершеннолетних (по результатам анализа переписок взрослых и детей в сети Интернет) / А.С. Медведева, Е.Г. Дозорцева // Психология и право. – 2019. – Т. 9. №4. – С. 161–173. EDN VHKAVY

5. Методические рекомендации по обеспечению государственных и муниципальных образовательных организаций, реализующих программы начального общего, основного общего, среднего общего и среднего профессионального образования, оптимальным и безопасным доступом к государственным, муниципальным и иным информационным системам, информационно-телекоммуникационной сети «Интернет» / Минпросвещения России, Минцифры России. – М., 2025. – 11 с.

6. В ОП предложили ввести идентификацию для доступа к контенту 18+ в интернете // РИА Новости. – 2025. – 21 окт. – URL: https://ria.ru/20251021/internet-2049496070.html (дата обращения: 16.02.2026).

7. Большинство подростков в России знают, как вести себя при кибербуллинге // ТАСС. – URL: https://tass.ru/obschestvo/11242357 (дата обращения: 16.02.2026).

8. Уголовный кодекс РФ. – URL: https://base.garant.ru/10108000/ (дата обращения: 16.02.2026).

9. О защите детей от информации, причиняющей вред их здоровью и развитию: Федеральный закон №436-ФЗ: принят 29 декабря 2010 года. – URL: http://kremlin.ru/acts/bank/32492 (дата обращения: 05.02.2026).

10. О персональных данных: Федеральный закон №152-ФЗ: принят 27 июля 2006 года: ред. от 14.07.2024. – URL: https://base.garant.ru/12148567/ (дата обращения: 01.02.2026).

11. Шпитцер М. Антимозг: цифровые технологии и мозг / М. Шпитцер. – М.: АСТ, 2013. – 288 с.