ЗАЩИТА ПРАВ ДЕТЕЙ В ЦИФРОВОМ ПРОСТРАНСТВЕ: КИБЕРБЕЗОПАСНОСТЬ И НЕПРИКОСНОВЕННОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

Ганиева Мадина Гофуровна

Студентка 1-го курса

Ташкентского государственного юридического университета

Дисциплина: Делопроизводство на государственном языке / Академическое письмо.

Телефон: +998 97 317-73-69

Аннотация. В статье рассматриваются актуальные вопросы защиты прав и законных интересов детей в условиях цифровой трансформации общества. Анализируются основные угрозы, возникающие в процессе использования детьми интернета, социальных сетей, онлайн-платформ и цифровых образовательных ресурсов. Особое внимание уделяется вопросам кибербезопасности, защите персональных данных несовершеннолетних, предупреждению кибербуллинга, интернет-мошенничества и распространения противоправного контента. Рассматриваются правовые основы защиты детей в цифровой среде, международные стандарты и национальные механизмы обеспечения информационной безопасности несовершеннолетних. Обосновывается необходимость совершенствования законодательства, повышения цифровой грамотности детей, родителей и педагогов, а также укрепления взаимодействия государства, семьи и образовательных учреждений.

Ключевые слова: права детей, цифровое пространство, кибербезопасность, персональные данные, конфиденциальность, интернет, кибербуллинг, цифровая грамотность, информационная безопасность, защита несовершеннолетних.

В современном мире цифровые технологии стали неотъемлемой частью повседневной жизни детей. Интернет, социальные сети, электронные

образовательные платформы, мобильные приложения и интерактивные ресурсы открывают широкие возможности для получения знаний, общения, творческого развития и самореализации несовершеннолетних.

Вместе с тем активное использование цифровых технологий сопровождается возникновением новых угроз для безопасности и прав детей. Среди наиболее распространённых проблем можно выделить распространение персональных данных без согласия, кибербуллинг, интернет-мошенничество, вовлечение несовершеннолетних в опасные онлайн-сообщества, доступ к вредоносному контенту и незаконное использование детских изображений.

Особую актуальность приобретает обеспечение права ребёнка на неприкосновенность частной жизни и защиту персональных данных. Дети не всегда способны самостоятельно оценивать возможные последствия публикации личной информации, фотографий, видеозаписей и сведений о своём местонахождении.

В этих условиях защита прав детей в цифровом пространстве становится важнейшей задачей государства, семьи, образовательных учреждений и общества в целом.

Целью данной статьи является исследование правовых и организационных механизмов защиты детей в цифровой среде, анализ основных угроз кибербезопасности и разработка предложений по обеспечению неприкосновенности персональных данных несовершеннолетних.

Понятие и основные особенности защиты прав детей в цифровом пространстве Цифровое пространство представляет собой совокупность информационных ресурсов, электронных платформ, социальных сетей, интернет-сервисов и технологических систем, посредством которых осуществляется обмен информацией и взаимодействие пользователей.

Для детей цифровая среда выполняет несколько важных функций:

- образовательную — предоставляет доступ к электронным учебникам, онлайн-курсам и образовательным платформам;

- коммуникативную — обеспечивает общение со сверстниками, учителями и родственниками;
- информационную — позволяет получать сведения о различных событиях и явлениях;
- развивающую — способствует формированию творческих, интеллектуальных и цифровых навыков;
- развлекательную — предоставляет доступ к играм, мультимедийному контенту и интерактивным приложениям.

Однако ребёнок в силу возраста и недостаточного жизненного опыта может не всегда правильно оценивать риски, связанные с использованием цифровых технологий. Поэтому защита его прав должна учитывать возрастные особенности, уровень цифровой грамотности и необходимость особых гарантий безопасности.

Важнейшими правами ребёнка в цифровом пространстве являются право на получение достоверной информации, образование, свободу выражения мнения, защиту от насилия и эксплуатации, неприкосновенность частной жизни и безопасность персональных данных.

При этом обеспечение безопасности не должно необоснованно ограничивать доступ детей к полезным образовательным и информационным ресурсам.

Основные киберугрозы, с которыми сталкиваются дети Одной из главных проблем современного цифрового общества является рост количества угроз, направленных на несовершеннолетних пользователей интернета.

Кибербуллинг. Представляет собой систематическое преследование, оскорбление, унижение или запугивание ребёнка посредством социальных сетей, мессенджеров, онлайн-игр и других цифровых платформ. Кибербуллинг может негативно влиять на психологическое состояние ребёнка, его самооценку, успеваемость и социальные отношения.

Интернет-мошенничество. Злоумышленники могут использовать поддельные страницы, фиктивные конкурсы, игровые предложения и сообщения для получения личной информации, паролей или денежных средств. Дети часто становятся

уязвимыми участниками подобных схем из-за недостаточного опыта распознавания мошеннических действий.

Фишинг. Это способ получения конфиденциальной информации посредством поддельных электронных писем, сообщений и интернет-сайтов. Ребёнок может случайно передать злоумышленникам данные своей учётной записи или информацию о семье.

Опасный интернет-контент. Несовершеннолетние могут сталкиваться с материалами, содержащими насилие, жестокость, пропаганду опасного поведения и другую информацию, способную отрицательно повлиять на их развитие.

Онлайн-груминг. Представляет собой установление доверительных отношений с ребёнком через интернет с целью последующей манипуляции, эксплуатации или совершения противоправных действий. Данная угроза требует особого внимания со стороны родителей и специалистов.

Незаконное распространение фотографий и видеоматериалов. Публикация изображений ребёнка без надлежащих правовых оснований и соблюдения его интересов может привести к нарушению права на частную жизнь, унижению достоинства и другим негативным последствиям.

Перечисленные угрозы показывают, что кибербезопасность детей должна рассматриваться как комплексная задача, включающая технические, правовые, образовательные и социальные меры.

Неприкосновенность персональных данных детей в цифровой среде

Персональные данные — это информация, которая позволяет прямо или косвенно идентифицировать конкретного человека. К персональным данным детей относятся:

- фамилия, имя и отчество;
- дата рождения;
- домашний адрес и номер телефона;
- фотографии и видеозаписи;
- сведения об образовательном учреждении;

- данные о местонахождении;
- сведения об учётных записях и цифровой активности;
- иная информация, позволяющая установить личность несовершеннолетнего.

Особую опасность представляет публикация персональных данных в открытом доступе. Например, размещение фотографий ребёнка с указанием его имени, школы, адреса проживания и местонахождения может создать условия для неправомерного использования данной информации.

Важной проблемой является также сбор данных цифровыми платформами и мобильными приложениями. Некоторые сервисы могут получать сведения о действиях пользователей, их интересах, предпочтениях и поведении в интернете.

Защита персональных данных детей должна основываться на следующих принципах:

1. Законность сбора и обработки персональных данных.
2. Ограничение сбора информации только необходимыми сведениями.
3. Обеспечение конфиденциальности и безопасности данных.
4. Недопущение незаконного распространения детских фотографий и видеозаписей.
5. Учет возраста ребёнка и его наилучших интересов.
6. Обеспечение доступных механизмов обращения и защиты нарушенных прав.

При использовании цифровых платформ необходимо учитывать не только согласие родителей или законных представителей в предусмотренных законом случаях, но и возрастную зрелость ребёнка, его мнение и право на уважение частной жизни.

Правовые основы защиты детей в цифровом пространстве Защита прав детей в цифровой среде основывается на международных и национальных нормативно-правовых актах.

Одним из основных международных документов является Конвенция ООН о правах ребёнка, принятая 20 ноября 1989 года. Она закрепляет фундаментальные права несовершеннолетних, включая право на защиту от всех форм насилия, право на частную жизнь, получение информации, образование и развитие.

Особое значение имеют следующие положения Конвенции:

- статья 3 — принцип наилучшего обеспечения интересов ребёнка;
- статья 13 — право ребёнка на свободу выражения мнения и получение информации;
- статья 16 — право на защиту от произвольного или незаконного вмешательства в личную жизнь;
- статья 17 — доступ к информации и материалам, направленным на содействие благополучию ребёнка;
- статья 19 — защита от всех форм физического или психологического насилия.

В Республике Узбекистан правовые гарантии защиты несовершеннолетних закреплены в Конституции Республики Узбекистан, Законе «О гарантиях прав ребёнка» и других нормативно-правовых актах.

Важное значение имеет также Закон Республики Узбекистан «О персональных данных» от 2 июля 2019 года № ЗРУ-547, регулирующий отношения, связанные со сбором, обработкой, хранением и защитой персональных данных.

Законодательство о защите детей должно применяться с учётом особенностей цифровой среды, в которой информация может быстро распространяться, копироваться и сохраняться даже после её удаления с первоначального ресурса.

Таким образом, эффективная защита несовершеннолетних требует не только наличия нормативных положений, но и действенных механизмов их практической реализации.

Роль семьи и образовательных учреждений в обеспечении кибербезопасности детей Важнейшую роль в формировании безопасного цифрового поведения ребёнка играют родители и образовательные учреждения.

Семья является первой средой, в которой ребёнок получает представление о правилах общения, личной безопасности и ответственности за собственные действия. Родители должны объяснять детям, почему нельзя передавать посторонним пароли, адрес проживания, номера телефонов и другие конфиденциальные сведения.

Вместе с тем чрезмерный контроль за цифровой активностью ребёнка не всегда способствует формированию самостоятельности. Поэтому родительское сопровождение должно сочетать разумный контроль, доверительное общение и обучение правилам безопасного поведения.

Образовательные учреждения также должны систематически проводить мероприятия по формированию цифровой грамотности.

К основным направлениям такой деятельности относятся:

- проведение занятий по основам кибербезопасности;
- обучение распознаванию мошеннических сообщений и интернет-угроз;
- формирование навыков безопасного использования социальных сетей;
- разъяснение правил защиты персональных данных;
- профилактика кибербуллинга;
- обучение ответственному поведению в цифровом пространстве;
- организация консультаций для родителей и педагогов.

Особенно важно включать вопросы цифровой безопасности в содержание воспитательной работы, информатики и других учебных дисциплин.

Основные направления совершенствования механизмов защиты детей в цифровой среде Для повышения эффективности защиты прав несовершеннолетних в условиях цифровой трансформации целесообразно реализовать комплекс правовых, организационных и образовательных мер.

Первое — совершенствование законодательства. Необходимо последовательно развивать нормативно-правовые механизмы, регулирующие обработку персональных данных детей, ответственность цифровых платформ и предупреждение противоправных действий в интернете.

Второе — повышение ответственности цифровых платформ. Следует совершенствовать механизмы выявления и ограничения распространения материалов, представляющих угрозу для несовершеннолетних, а также обеспечивать доступные процедуры подачи жалоб.

Третье — развитие цифровой грамотности. Необходимо формировать у детей практические навыки безопасного поведения в интернете, защиты личной информации и критической оценки цифрового контента.

Четвёртое — усиление родительского и педагогического сопровождения. Следует организовывать образовательные программы для родителей и педагогов, направленные на распознавание интернет-угроз и оказание помощи детям.

Пятое — совершенствование механизмов реагирования. Важно обеспечить доступные способы сообщения о кибербуллинге, онлайн-мошенничестве, эксплуатации и других нарушениях прав несовершеннолетних.

Шестое — внедрение технологий защиты. Использование безопасных настроек конфиденциальности, родительского контроля, многофакторной аутентификации и современных средств киберзащиты может существенно снизить риски неправомерного доступа к данным детей.

Седьмое — развитие международного сотрудничества. Поскольку цифровые угрозы не ограничиваются государственными границами, необходимо укреплять взаимодействие государств, международных организаций и технологических компаний в сфере защиты несовершеннолетних.

ЗАКЛЮЧЕНИЕ

В условиях цифровой трансформации защита прав детей в интернете приобретает особое социальное и правовое значение. Цифровые технологии предоставляют несовершеннолетним широкие возможности для получения образования, общения и развития, однако одновременно создают новые риски, связанные с кибербуллингом, интернет-мошенничеством, незаконным распространением персональных данных и доступом к опасному контенту.

Проведённый анализ показывает, что обеспечение кибербезопасности детей должно основываться на комплексном подходе, объединяющем правовое регулирование, техническую защиту, цифровое образование и ответственное участие семьи.

Особое внимание необходимо уделять неприкосновенности персональных данных несовершеннолетних, поскольку информация о ребёнке может использоваться в противоправных целях и причинять ему длительный вред.

В связи с этим совершенствование законодательства, повышение ответственности цифровых платформ, развитие цифровой грамотности и укрепление взаимодействия государства, семьи и образовательных учреждений являются важнейшими условиями обеспечения безопасности детей в цифровом пространстве.

Таким образом, цифровая среда должна быть не только пространством получения информации и общения, но и безопасной средой, в которой гарантируются достоинство, частная жизнь, свобода и законные интересы каждого ребёнка.

ЛИТЕРАТУРЫ

1. Конвенция ООН о правах ребёнка от 20 ноября 1989 года. URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

2. Конституция Республики Узбекистан. Новая редакция, принятая на референдуме 30 апреля 2023 года. URL: https://constitution.uz/ru

3. Закон Республики Узбекистан от 2 июля 2019 года № ЗРУ-547 «О персональных данных». URL: https://lex.uz/docs/4396428

4. Закон Республики Узбекистан «О гарантиях прав ребёнка» от 7 января 2008 года № ЗРУ-139. URL: https://lex.uz/docs/1297315

5. UNICEF. *The State of the World's Children 2017: Children in a Digital World.* New York: UNICEF, 2017. URL: https://www.unicef.org/reports/state-worlds-children-2017

6. UNICEF. *Guidance on AI and Children, Version 3.0.* 2021. URL: https://www.unicef.org/globalinsight/reports/policy-guidance-ai-children

7. UNICEF. *Child Online Protection.* URL: https://www.unicef.org/protection/violence-against-children-online

8. International Telecommunication Union (ITU). *Guidelines for Parents and Educators on Child Online Protection.* URL: https://www.itu.int/cop/

9. World Health Organization (WHO). *Violence Against Children.* URL: https://www.who.int/news-room/fact-sheets/detail/violence-against-children