УДК 377.8

Новикова Д.Д.
Поволжский государственный университет
телекоммуникаций и информатики, Самара

ОСНОВНЫЕ УГРОЗЫ ДЛЯ ДЕТЕЙ В ИНТЕРНЕТЕ И СПОСОБЫ ЗАЩИТЫ

Аннотация. В статье рассматриваются ключевые угрозы, с которыми сталкиваются дети в информационном пространстве: кибербуллинг, вредоносный контент, вовлечение в незаконную деятельность и интернет-зависимость. Описаны основные методы защиты детей: правовое регулирование, технические средства, развитие цифровой грамотности,

психологическая поддержка и сотрудничество между государственными структурами, бизнесом и гражданским обществом. Проведен анализ актуальной статистики. Сделаны выводы о необходимости комплексного подхода к обеспечению безопасности детей в сети Интернет.

Ключевые слова: безопасность детей, информационное пространство, интернет-угрозы, цифровая грамотность, кибербуллинг, родительский контроль.

Информационные технологии прочно вошли в повседневную жизнь детей, предоставляя широкие возможности для обучения, общения и досуга. Однако вместе с позитивными аспектами возрастают и риски негативного воздействия цифровой среды. По данным Лаборатории Касперского, в 2024 г. 60 % детей сталкивались с нежелательным контентом в интернете, а около 30 % подвергались кибербуллингу. В связи с этим возрастает необходимость изучения основных угроз и способов защиты детей в информационном пространстве. Рассмотрим наиболее популярные из них.

Кибербуллинг – это систематическое использование электронных средств для нанесения вреда другим пользователям. Для детей кибербуллинг особенно опасен тем, что унижения и оскорбления распространяются быстро, на широкую аудиторию, и их трудно удалить. Исследования показывают, что жертвами кибербуллинга часто становятся дети с низкой самооценкой или слабо выраженными социальными навыками, что приводит к депрессии, тревожным расстройствам и даже суицидальным мыслям.

По данным ВЦИОМ (2024), 25 % подростков в России признались, что хотя бы раз подвергались кибербуллингу, а 7 % сталкивались с этим регулярно [1]. Особую обеспокоенность вызывает факт, что многие дети скрывают факты травли от родителей и педагогов, опасаясь осуждения или усиления травли. Дети становятся удобной целью мошенников по нескольким причинам: доверчивость, стремление к быстрым результатам (победе в игре, популярности в соцсетях) и отсутствие навыков распознавания угроз. Распространенные схемы: обман о выигрыше в конкурсах, фальшивые предложения «быстрых заработков», просьбы перевести деньги «другу в беде», фишинговые письма с зараженными ссылками.

Исследование Positive Technologies показывает, что около 12 % детей в возрасте от 10 до 15 лет хотя бы раз становились жертвами попыток онлайн-мошенничества, причем в 4 % случаев мошенникам удавалось получить личные данные или деньги [2].

Интернет-зависимость характеризуется патологическим стремлением ребенка проводить чрезмерное количество времени онлайн за счет сна, учебы, физической активности и реального общения. Наиболее подвержены дети и подростки, испытывающие дефицит эмоциональных связей в реальной жизни.

Формы проявления интернет-зависимости: бессонница, тревожность при невозможности выйти в сеть, потеря интереса к учебе и хобби, нарушения пищевого поведения.

Совокупный анализ данных различных исследований (Лаборатория Касперского, ВЦИОМ, Positive Technologies, Лига безопасного интернета) позволяет сделать вывод, что: более 65 % детей в возрасте от 8 до 16 лет в России хотя бы раз сталкивались с интернет-угрозами различного характера. Из них:

- 27 % стали жертвами кибербуллинга,
- 53 % сталкивались с вредоносным контентом,
- 12 % становились объектами мошеннических действий,
- 17–18 % проявляли признаки интернет-зависимости.

Эти цифры подчеркивают масштаб проблемы и необходимость комплексного подхода к обеспечению безопасности детей в цифровом пространстве. Стоит отметить, что ключевую роль в создании безопасной цифровой среды для детей играют правовые меры. На международном уровне защита детей в интернете обеспечивается Конвенцией ООН о правах ребенка. В России действует ряд нормативных актов:

- Федеральный закон № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Постановление Правительства РФ № 1101 об ограничении доступа к запрещенной информации.

Эти документы закрепляют ответственность владельцев сайтов и операторов связи за распространение запрещенной информации и позволяют оперативно блокировать опасные ресурсы [3].

Кроме того, с 2021 г. в России активно развивается практика маркировки контента по возрастным категориям и применения «реестра запрещенных сайтов» (Роскомнадзор).

Технические инструменты создают дополнительный барьер на пути вредоносного контента:

- фильтрация трафика (например, через «семейные» DNS-серверы типа Yandex.DNS);
- родительский контроль в устройствах и приложениях (настройка лимитов времени, блокировка приложений);
- антивирусные решения с функцией веб-контроля, защищающие от фишинга и вредоносных ссылок;
- мониторинг активности: специальные программы позволяют родителям видеть, какие сайты посещает ребенок и сколько времени он проводит в сети.

Современные системы, такие как Kaspersky Safe Kids или Norton Family, предлагают не только блокировку контента, но и отчеты об активности, уведомления о выходе за пределы разрешенного времени, а

также контроль над геолокацией ребенка. Однако важно понимать: технические средства являются вспомогательным инструментом и не заменяют воспитательные меры.

Развитие критического мышления и цифровой грамотности среди детей и родителей является важнейшей долгосрочной стратегией защиты.

Необходимо обучать детей:

- различать достоверные и фальшивые источники информации;
- осознавать риски публикации личных данных в интернете;
- правильно реагировать на случаи угроз и кибербуллинга (не вступать в диалог, сохранять доказательства, обращаться за помощью).

Организация уроков цифровой безопасности в школах, проведение тренингов для родителей и создание обучающих онлайн-курсов доказали свою эффективность.

По данным проекта «Урок цифры» Минцифры России, участие в образовательных инициативах в 2024 г. приняли более 2,5 млн школьников [4].

Эффективная защита детей требует комплексного подхода:

- государство должно создавать законодательную базу и развивать инфраструктуру фильтрации контента;
- бизнес – в первую очередь IT-компании и разработчики приложений – обязан внедрять встроенные механизмы защиты (например, автоматическое ограничение возрастного доступа);
- гражданские организации должны проводить кампании по повышению осведомленности, поддерживать просветительские инициативы, обеспечивать общественный контроль.

Успешные примеры включают кампанию «Безопасный интернет» от Лиги безопасного интернета и международные проекты типа WePROTECT Global Alliance.

Таким образом, обеспечение безопасности детей в информационном пространстве требует многоуровневого взаимодействия всех заинтересованных сторон: родителей, педагогов, государства, бизнеса и самих детей. Статистические данные свидетельствуют о серьезности проблемы, но эффективное применение правовых, технических, образовательных и психологических мер позволяет значительно снизить риски.

Формирование культуры ответственного и осознанного пользования интернетом с раннего возраста должно стать приоритетной задачей на уровне государственной политики и образовательных программ.

Список использованных источников:

1. Детский кибербуллинг и как с ним бороться // ВЦИОМ Новости: [сайт]. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/detskii-kiberbulling-i-kak-s-nim-borotsja (дата обращения: 28.04.2025).

2. Новое исследование Positive Technologies // Cyber Media: [сайт]. URL: https://securitymedia.org/news/novoe-issledovanie-positive-technologies-

bolee-treti-izuchennykh-sim-kart-dayut-vozmozhnost-dlya-pop.html (дата обращения: 28.04.2025).

3. Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 30.11.2024) «О защите детей от информации, причиняющей вред их здоровью и развитию» // КонсультантПлюс: [сайт]. URL: https://www.consultant.ru/document/cons_doc_LAW_108808/d44bdb356e6a691d0c72fef05ed16f68af0af9eb/ (дата обращения: 28.04.2025).

4. Новый сезон «Урока Цифры» // Национальные проекты РФ: [сайт]. URL: https://национальныепроекты.рф/news/v-novom-sezone-uroka-tsifry-prinyali-uchastie-bolee-2-5-mln-shkolnikov/ (дата обращения: 28.04.2025).

Novikova D.D.
Volga Region State University of
Telecommunications and Informatics, Samara

THE MAIN THREATS TO CHILDREN ON THE INTERNET AND WAYS TO PROTECT THEM

Abstract. The article examines the key threats faced by children in the information space: cyberbullying, malicious content, involvement in illegal activities and Internet addiction. The main methods of child protection are described: legal regulation, technical means, development of digital literacy, psychological support and cooperation between government agencies, business and civil society. The analysis of current statistics is carried out. Conclusions are drawn about the need for an integrated approach to ensuring the safety of children on the Internet.

Keywords: child safety, information space, Internet threats, digital literacy, cyberbullying, parental control.