



ISSN: 2181-9416

YURIST AXBOROTNOMASI

ВЕСТИНИК ЮРИСТА * LAWYER HERALD

HUQUQIY, IJTIMOIIY, ILMIY-AMALIY JURNAL



CYBERLENINKA

НАУЧНАЯ ЭЛЕКТРОННАЯ
БИБЛИОТЕКА
LIBRARY.RU

GULIMOV Amanlik BazarbaevichBerdaq nomidagi Berdaq nomidagi Qoraqalpoq davlat universiteti
“Inson huquqlari, davlat huquqi va boshqaruvi” kafedrası professori, y.f.d.E-mail: gamanlik75@mail.ru**Kitaybekova Malika Salauat qizi**

Berdaq nomidagi Qoraqalpoq davlat universiteti magistranti

E-mail: malikakitaybrkova01@gmail.com

RAQAMLI MAKONDA BOLANING XAVFSIZLIK HUQUQINI AMALGA OSHIRISHDAGI MUAMMOLAR

ANNOTATSIYA

Raqamlashtirish va internetning globallasuvi sharoitida onlayn muhitda bolalarni himoya qilish asosiy huquqiy muammolardan biriga aylanmoqda. Maqola jamiyatni raqamlashtirish va onlayn muhit bilan bog'liq tahdidlarning kuchayishi sharoitida bolalarning raqamli xavfsizligini ta'minlash muammosini o'rganishga bag'ishlangan. Tadqiqotning maqsadi raqamli makonda bola huquqlarini himoya qilishni tartibga soluvchi xalqaro va milliy qonunchilikni tahlil qilish, shuningdek, O'zbekiston Respublikasining huquqiy bazasini takomillashtirish bo'yicha tavsiyalar ishlab chiqishdan iborat.

Tadqiqot davomida kibertahdidlarni tartibga solish va oldini olishning rivojlangan tizimiga ega bo'lgan Buyuk Britaniya va Finlyandiyaning me'yoriy modellari qiyosiy tahlil qilindi. Ishning ilmiy yangiligi huquqiy normalar va himoya qilishning institutsional mexanizmlarini tizimlashtirish, O'zbekiston Respublikasi qonunchiligidagi bo'shliqlarni aniqlash va bolalarning raqamli xavfsizligi to'g'risida alohida qonun qabul qilish zarurligini asoslash bilan ifodalanadi.

Amaliy natijalar sifatida raqamli savodxonlik bo'yicha ta'lim modullarini joriy etish, idoralararo muvofiqlashtiruvchi organi tashkil etish, raqamli qo'llab-quvvatlash maktab jamoalarini shakllantirish va xalqaro standartlarni milliy qonunchilikka integratsiya qilish bo'yicha kompleks chora-tadbirlar taklif etildi. Bundan kelib chiqadigan xulosa shuki, raqamli makonda bolalarni himoya qilish huquqiy, ta'limiy va profilaktik mexanizmlarni birlashtirgan holda tizimli yondashuvni talab qiladi.

Kalit so'zlar: bola huquqlari, kiberjinoyatlar, kiberhujum, internet tahdidlari, raqamli xavfsizlik, milliy qonunchilik, raqamli platformalar, xalqaro standartlar, raqamli huquqlar.

AMANLIK GulimovProfessor of the Department of Human Rights, State Law and Administration
at Berdakh Karakalpak State University, Doctor of Juridical SciencesE-mail: gamanlik75@mail.ru**MALIKA Kitaybekova**

Master's student at Karakalpak

State University named after Berdakh

E-mail: malikakitaybrkova01@gmail.com

PROBLEMS IN THE IMPLEMENTATION OF THE CHILD'S RIGHT TO SAFETY IN THE DIGITAL SPACE

ANNOTATION

In the context of digitalisation and the globalisation of the internet, ensuring the online safety of children has become one of the key legal issues. This article examines the issue of ensuring children's digital security in a digitalised society, where there are increasing threats associated with the online environment. The study aims to analyse international and national legislation that regulates the protection of children's rights in the digital space, and to develop recommendations for improving the legal framework in the Republic of Uzbekistan.

During the study, a comparative analysis of the regulatory models of Great Britain and Finland — countries with well-developed systems for regulating and preventing cyber threats — was conducted. The scientific novelty of the study lies in the systematisation of legal norms and institutional protection mechanisms, the identification of gaps in Republic of Uzbekistan legislation, and the justification of the need to adopt a separate law on digital child safety.

Practical results include the proposal of comprehensive measures: the introduction of educational modules on digital literacy; the creation of an interdepartmental coordination body; the formation of school digital support teams; and the integration of international standards into national legislation. In conclusion, protecting children in the digital space requires a systematic approach combining legal, educational and preventive mechanisms.

Keywords: child rights, cybercrime, cyberbullying, internet threats, digital security, national legislation, digital platforms, international standards, digital rights.

В настоящее время, в условиях интенсивного развития цифровизации, перехода к цифровому формату взаимодействия, влияющего на все сферы жизни, всё большее значение приобретает обеспечение прав ребёнка в виртуальной среде.

На глобальном уровне интернет стал неотъемлемой частью жизни, особенно для несовершеннолетних, предоставляя широкие возможности для обучения, общения, досуга и творчества, вследствие чего дети становятся полноправными участниками цифрового пространства с раннего возраста. Однако вместе с этим в научной литературе обозначается острая полемика относительно баланса между предоставлением детям свободы доступа к информации и необходимостью их защиты от угроз.

Одни исследователи (Livingstone, 2018) подчёркивают, что признание ребёнка полноценным субъектом цифровых прав предполагает недопустимость чрезмерных ограничений, поскольку именно свободный доступ обеспечивает развитие личности и социализацию [1]. В то же время другие авторы (Kibby and Helsper, 2020) обращают внимание на то, что именно бесконтрольный доступ становится причиной кибербуллинга, онлайн-эксплуатации, распространения деструктивного контента и вовлечения в противоправную деятельность [2]. Дополняет данную дискуссию вторая полемика, связанная с тем, какой автор должен играть ключевую роль в обеспечении цифровой безопасности детей – государство или сами интернет-платформы. Сторонники государственного регулирования (Staksrud, 2017) утверждают, что только через правовые механизмы можно создать эффективные гарантии защиты детей от цифровых угроз [3]. В противоположность этому, ряд исследователей (Gillespie, 2019) настаивают, что чрезмерная роль государства приведёт к цензуре и ограничению свободы слова, а эффективной стратегией является развитие саморегуляции платформ и цифровой грамотности пользователей [4].

Тут можно отметить, что в центре научной повестки оказываются сразу две ключевые дилеммы:

- 1) Где проходит граница между свободой ребёнка в интернете и необходимостью его защиты;
- 2) Кто должен нести главную ответственность за обеспечение цифровой безопасности – государство или сами технологические компании.

Несомненно, решение этих вопросов требует адекватного правового регулирования как на национальном, так и на международном уровнях, а также координации усилий государства, частного сектора и институтов гражданского общества.

Безусловно, представленная полемика отражает сложность и многогранность вопросов, связанных с участием несовершеннолетних в цифровом пространстве. Мы частично согласны с взглядами Livingstone (2018), поскольку признаём, что свободный и необременённый

чрезмерными ограничениями доступ к информации является фундаментальным для полноценного развития личности ребёнка и его социализации в современном обществе. В то же время, считаем необходимым учитывать аргументы Kibby и Helsper (2020), которые акцентируют внимание на реальных угрозах, возникающих вследствие бесконтрольного доступа, таких как кибербуллинг, эксплуатация и распространение вредоносного контента, что требует эффективных мер защиты.

Аналогично, признаём значимость позиций Staksrud (2017), подчёркивающих роль государства в создании правовых механизмов, обеспечивающих системные гарантии безопасности детей в цифровой среде. Вместе с тем, мы считаем оправданным внимание Gillespie (2019) к рискам чрезмерного государственного регулирования, которое может привести к цензуре и ограничению свободы слова, а также к необходимости развития механизмов саморегуляции интернет-платформ и повышения цифровой грамотности пользователей.

Таким образом, мы разделяем мнение о том, что решение двух ключевых дилемм – установления баланса между свободой ребёнка и необходимостью его защиты, а также определения ответственного за цифровую безопасность субъекта – возможно лишь при условии комплексного подхода, включающего адекватное национальное и международное правовое регулирование, а также координацию усилий всех заинтересованных сторон: государства, частного сектора и гражданского общества. Такой подход позволяет обеспечить эффективную защиту прав и свобод несовершеннолетних в цифровом пространстве, учитывая при этом их интересы и права как субъекта цифровой среды.

На сегодняшний день, Международное сообщество активно адаптирует правовые механизмы к вызовам цифровой эпохи, уделяя особое внимание защите прав детей в онлайн-среде. Ключевым международным актом в этой сфере является Конвенция ООН о правах ребёнка (1989 г.), положения которой, несмотря на её принятие до наступления цифровой эры, остаются актуальными и применимыми к современным реалиям информационного общества (ратифицирована Республикой Узбекистан от 9 декабря 1992 г.). Ряд её статей напрямую соотносится с проблемами цифровой безопасности:

- статья 17 устанавливает право ребёнка на доступ к достоверной информации, а также обязательства государства по обеспечению ей качества и безопасности;
- статья 19 предписывает защиту детей от всех форм насилия, включая психологическое, а также охватывает, в частности, кибербуллинг и онлайн-преследование;
- статья 34 направлена на предупреждение сексуальной эксплуатации, включая случаи, происходящие через интернет и цифровые платформы[5].

Существенным шагом в признании цифровой среды частью жизненного пространства ребёнка стало принятие в 2021 году Общего замечания №25 Комитета ООН по правам ребёнка. Данный документ выделяет не только право ребёнка на участие в цифровом пространстве, но и необходимость обеспечения его защиты от рисков, связанных с интернетом. Основные положения замечания включают:

- необходимость учитывать интересы ребёнка при проектировании цифровых сервисов и платформ;
- обязанность государств регулировать деятельность частных цифровых компаний, включая провайдеров и владельцев социальных сетей;
- требование к прозрачности алгоритмов, которые могут воздействовать на эмоциональное состояние и поведение детей [6].

Следует отметить, что дополнительным международным документом выступает **Стратегия Совета Европы по правам ребёнка на 2022-2027 годы**, где цифровая безопасность детей рассматривается как отдельный приоритет [7]. Наряду с этим, **Общий регламент Европейского союза по защите данных (GDPR)** устанавливает особые правила для обработки персональных данных несовершеннолетних, усиливая ответственность платформ и сервисов за цифровую безопасность [8].

Как нам известно, международные нормы всё в большей степени рассматривают цифровую сферу как неотъемлемую часть жизни ребёнка, обязывая государства формировать действенные правовые и институциональные механизмы защиты прав несовершеннолетних в условиях цифровизации.

В последние годы Республика Узбекистан предпринимает действенные меры по реформированию законодательства в области прав человека, уделяя особое внимание обеспечению прав и интересов ребёнка. Однако правовое регулирование вопросов, связанных с обеспечением безопасности несовершеннолетних в цифровой среде, остаётся недостаточно разработанным и носит фрагментарный характер [9].

В Конституции Республики Узбекистан ребёнок признаётся в качестве полноценного носителя правового статуса. В частности, статья 78 возлагает на государство обязанность по охране материнства и детства, а статья 33 гарантирует каждому свободу получения и распространения информации, а также защиту персональных данных [10]. Однако на наш взгляд, несмотря на то, что в Основном законе прямо не обозначается категория цифровой безопасности, это свидетельствует не столько о пробеле, сколько о необходимости дальнейшего развития национального законодательства с учётом современных вызовов цифровой среды.

К числу нормативно-правовых актов Узбекистана, прямо или косвенно затрагивающих вопросы защиты детей в цифровом пространстве, относятся следующие:

- **Закон «О гарантиях прав ребёнка»** от 7 января 2008 года, в котором содержится перечень основных прав несовершеннолетних, включая защиту от всех форм насилия и жестокого обращения. Вместе с тем, вопросы, связанные с цифровыми угрозами, в законе представлены в нераскрытом виде [11].

- **Закон «О персональных данных»** от 2 июля 2019 года регулирует порядок сбора, обработки и хранения персональных данных, включая данные несовершеннолетних. Однако в нём отсутствует положения, касающиеся возрастного ценза, обязательного согласия родителей или механизмов защиты цифровых прав детей, аналогичных тем, что закреплены, например, в Регламенте ЕС 2016/679 (GDPR) [12,13].

- **Закон «Об информатизации»** (2024 г.) и **Закон «О средствах массовой информации»** (1997 г.) содержит положения, запрещающие распространение информации, вредящей здоровью и нравственности граждан, но при этом не делают акцента на защите детей от цифровых рисков [14,15].

На наш взгляд, существенным шагом в направлении признания онлайн-угроз стало присоединение Узбекистана в 2021 году к **Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуального насилия (Лансаротской конвенции)**, предусматривающей в том числе меры защиты детей в интернете [16].

Несмотря на обозначенные позитивные изменения, система законодательства Узбекистана сталкивается с рядом структурных проблем:

- отсутствие отдельного закона, регулирующего цифровые права и безопасность детей в интернете;

- слабое регулирование деятельности цифровых платформ и социальных сетей, где происходят случаи кибербуллинга, онлайн-эксплуатации и распространения вредоносной информации;

- недостаточная развитость механизмов возрастной маркировки и ограничения доступа к контенту;

- низкий уровень цифровой грамотности среди родителей, педагогов и представителей правоохранительных органов, что ограничивает возможности превенции и правоприменения [17].

Как справедливо отмечает Бородин К.В., проблема обеспечения информационной безопасности несовершеннолетних осложняется тем, что Интернет является глобальной информационной средой, однако применяемые юридические механизмы обычно ограничены национальными рамками [18].

По мнению Кучма В.Р, социальные меры, направленные на защиту прав и свобод несовершеннолетних в цифровом пространстве, должны осуществляться целым рядом субъектов: родителями, педагогами, специально созданными организациями. К социальным мерам обеспечения информационной безопасности несовершеннолетних относятся создание и внедрение программ обучения детей и подростков правилам безопасного поведения в интернет-пространстве, профилактики интернет-зависимости, предупреждения рисков вовлечения в противоправную деятельность [19].

Данная задача представляется актуальной прежде всего для образовательных учреждений. Большинство учебников по информатике базового уровня формирует у учащихся неполную базу личной информационной безопасности в современной информационной среде. Так, в них не рассматриваются вопросы, связанные с навыками фильтрации нежелательного контента в Интернете, противодействия деструктивным программам, фишингу, психологическим преследованиям в Сети, а также касающиеся профилактики интернет-зависимости у детей. Это может негативно повлиять на психологическое и нравственное здоровье школьников [20].

Вышеприведённые мнения учёных даёт нам право, что при наличии базовой нормативно-правовой базы в сфере защиты прав ребёнка, её адаптации к вызовам цифровой эпохи требует системной модернизации, включая принятие специализированных актов, разработку правовых механизмов регулирования цифровой среды и развитие программ цифрового просвещения. Бесспорно, что наличие нормативной базы само по себе не гарантирует эффективную защиту ребёнка – это лишь один из необходимых элементов.

Хотя, К.Уолден (2020) справедливо подчеркивает важность правового регулирования, многие исследователи отмечают ограниченность исключительно законодательного подхода [21]. Так, Л. Хоффман (Hoffman, 2021) указывает, что одни лишь законы не способны защитить ребёнка от реальных угроз цифровой среды, если отсутствуют знания и навыки безопасного поведения [22]. В условиях высокой динамики цифровых технологий нормативные акты зачастую не успевают адаптироваться к новым вызовам. В то же время чрезмерное упование на образовательную профилактику, как её описывает И.Абдуллаева (2022), также вызывает сомнения [23]. По мнению Т. Мартинса (Martins, 2019), образовательные программы без надлежащего юридического обеспечения могут оставаться декларативными и не обеспечивать должной защиты в случаях, когда требуется правовая ответственность [24].

Таким образом, дискуссия не сводится к выбору «или–или». Более оправданным решением является комплементарный подход, где правовые акты создают базовую защиту, а образовательная профилактика наполняет её реальным содержанием, формируя устойчивую культуру цифровой безопасности. Практическое применение законодательства в области

цифровой безопасности в Узбекистане сталкивается с рядом системных и институциональных трудностей, которые существенно снижают эффективность правовых механизмов защиты детей.

Представленные в научной литературе позиции авторов убедительно демонстрирует, что обеспечение цифровой безопасности детей не может быть сведено к доминированию одного из подходов – исключительно правового или исключительно образовательного. Мы частично согласны с К.Уолденом (2020), подчёркивающим необходимость нормативного регулирования как основы функционирования системы цифровой защиты. Действительно, правовые акты обеспечивают формализацию обязательств и механизмов ответственности, без которых невозможно эффективное вмешательство в случаях нарушения прав ребёнка. Однако, как справедливо отмечают Л.Хоффман (2021) и Т.Мартинс (2019), одного только законодательного вмешательства недостаточно: при отсутствии цифровой грамотности и культуры безопасного поведения правовые нормы могут оставаться неэффективными или применяться постфактум, когда вред уже нанесён. В то же время мы разделяем и критику И.Абдулалаевой, указывающей на уязвимость исключительно образовательного подхода: в отсутствие нормативной поддержки профилактические меры могут носить декларативный характер и не гарантировать защиту в правовом смысле.

Таким образом, наиболее обоснованным представляется комплементарный подход, при котором правовое регулирование и образовательные инициативы взаимно дополняют друг друга: первое формирует институциональные рамки и ответственность, второе – способствует формированию цифровой компетентности и снижению рисков. Особенно актуален этот вывод в Республике Узбекистан, где, несмотря на формирование законодательной базы, реализация правовых норм сталкивается с институциональными ограничениями и недостаточной межведомственной координацией. Это подтверждает необходимость комплексного подхода, сочетающего правовые, образовательные и административные меры в целях устойчивого обеспечения цифровой безопасности несовершеннолетних.

Одной из наиболее острых проблем, как выше отметили является недостаточный уровень цифровой и правовой грамотности среди педагогов, сотрудников правоохранительных органов, органов опеки и попечительства, а также родителей. Это приводит к тому, что случаи кибербуллинга, онлайн-груминга и вовлечения несовершеннолетних в противоправную деятельность через интернет зачастую либо остаются незамеченными, либо воспринимаются как не представляющие угрозы.

Кроме того, в Узбекистане отсутствуют унифицированные методические рекомендации для органов, ответственных за защиту прав детей, по вопросам реагирования на угрозы в цифровой среде. Расследование интернет-преступлений в отношении несовершеннолетних осложняется рядом факторов, включая анонимность правонарушителей, использование зарубежных онлайн-платформ и отсутствие локальных центров мониторинга цифровых угроз.

Хочется отметить, что система профилактики и раннего вмешательства в стране в основном ориентирована в офлайн-угрозы. При этом официальные образовательные программы по цифровой безопасности в школах отсутствуют, в учебных планах нет обязательных модулей по этой теме, а системный анализ цифрового поведения детей, в том числе в социальных сетях, не применяется для выявления эмоционально уязвимых несовершеннолетних. Популярными среди подростков цифровые платформы и приложения (такие как YouTube, Telegram и TikTok) не подлежат национальному регулированию и не несут достаточной ответственности

за размещённый контент. В большинстве случаев государственные органы реагируют лишь постфактум, после возникновения негативных последствий.

Также наблюдается слабая координация между министерствами образования, внутренних дел, юстиции и агентствами, занимающимися цифровым развитием. В стране отсутствует единый координационный орган, уполномоченный обеспечивать защиту прав ребёнка в цифровом пространстве, что ведёт к фрагментарности мер, неэффективному мониторингу и отсутствию системной профилактики.

В качестве примера успешной зарубежной практики по цифровой безопасности детей целесообразно рассмотреть модель регулирования *Великобритании и Финляндии*. В *Великобритании* внедрена модель комплексного регулирования и цифрового образования через «UK Online Safety Bill» и инициативу «Education for a Connected World». *Великобритания* реализует системный подход к защите детей в цифровом пространстве, сочетая правовое регулирование, межведомственное сотрудничество и образовательные меры:

- **Онлайн-безопасность на законодательном уровне**, то есть принятый в 2023 году *Online Safety Act* возлагает на цифровые платформы юридическую обязанность защищать несовершеннолетних от вредоносного контента (включая кибербуллинг, груминг, контент о саморазрушительном поведении и т.д.). Закон требует от платформ проводить регулярные оценки рисков, модерировать контент и отчитываться перед регулирующим органом – Ofcom [25]. Компании, не выполняющие требования, могут быть оштрафованы на суммы до 10% от годового мирового оборота.

- **Образовательные инициативы**, то есть Министерство образования совместно с UK Council for Internet Safety (UKCIS) разработало программу *Education for a Connected World*, которая представляет собой национальные рекомендации по формированию цифровой грамотности у детей от дошкольного до старшего школьного возраста. Эти рекомендации включены в учебные планы и касаются вопросов конфиденциальности, киберэтикета, критического мышления и защиты от онлайн-угроз [26].

- **Межведомственное сотрудничество и координация**, то есть Великобритания создала специальную структуру – UKCIS, в которую входят представители правительственных ведомств, технологических компаний, образовательных учреждений и общественных организаций. Эта платформа обеспечивает постоянную координацию усилий в области онлайн-безопасности детей.

Анализ британского опыта в сфере цифровой безопасности несовершеннолетних позволяет обоснованно рекомендовать внедрение его ключевых элементов в нормативно-правовую и институциональную практику Узбекистана с адаптацией к действующим правовым и социальным условиям страны. В данном направлении представляется целесообразным:

- 1) Разработать и внедрить национальный правовой акт о цифровой безопасности, обязывающий онлайн-платформы защищать несовершеннолетних;
- 2) Ввести обязательный модуль по цифровой грамотности в школьные программы всех уровней, адаптируя подход *Education for a Connected World*;
- 3) Создать межведомственный координационный совет по цифровой безопасности детей с участием представителей IT-сектора, образования, Министерство внутренних дел, Министерство юстиции и негосударственных некоммерческих организаций.

Изучив практику *Финляндии* по цифровой безопасности детей, то можно увидеть, что в Финляндии профилактика цифровых рисков осуществляется через образование и психологическую поддержку. *Финляндия* признана одной из стран с наиболее безопасной

цифровой средой для детей благодаря целостному подходу, которой включает образовательные реформы, профилактику ментальных рисков и широкое вовлечение всех участников воспитательного процесса. В частности,

- Обязательное цифровое образование с начальной школы, то есть Финская школьная система включает элементы цифровой грамотности и безопасного поведения в интернете с первого класса. Темы варьируются от защиты личных данных до распознавания кибербуллинга и дезинформации. Обучение проводится не только через ИКТ-уроки (информационно-коммуникационные технологии), но и интегрировано в обществознание, литературу и даже искусство [27].

- Подготовка педагогов и школьных психологов, то есть учителя и школьные психологи проходят обязательную подготовку по вопросам цифровой безопасности и раннего выявления признаков психологической уязвимости у детей. Это позволяет своевременно вмешиваться при признаках тревожности, изоляции, возможного вовлечения в деструктивные онлайн группы [27].

- Механизм школьных команд реагирования (Digital Wellbeing Teams), то есть в каждой школе действуют междисциплинарные команды (включающие преподавателя, психолога, представителя родителей и IT-специалиста), которые отвечают за продвижение цифрового благополучия и реагирование на инциденты. Такие команды тесно сотрудничают с муниципальными и национальной службой поддержки детей (Mannerheim League for Child Welfare) [28].

Применительно к Узбекистану анализ зарубежной практики, в частности финской, позволяет выделить приоритетные сферы правового и организационного воздействия: внедрение цифрового образования, повышение квалификации педагогов и психологов, а также формирование школьных команд цифровой поддержки. В указанных направлениях представляется целесообразным рекомендовать следующие меры:

- 1) **Внедрить цифровое образование с младших классов** как часть базовой грамотности: не только технические навыки, но и этика, безоасность, распознавание онлайн-рисков;

- 2) **Обязательное обучение педагогов и школьных психологов** по вопросам цифровой безопасности и мониторинга эмоционального состояния детей;

- 3) **Создание школьных команд цифровой поддержки**, в которые будут входить педагоги, IT-специалисты и психологи, с регулярной координацией с местными органами образования.

Исходя из вышеприведённых примеров, считаем целесообразным из зарубежной практики провести сравнительный анализ текущей ситуацией в Узбекистане и моделью Великобритании и Финляндии в сфере цифровой безопасности детей в виде таблицы:

Компонент	Узбекистан	Великобритания	Финляндия
Закон о цифровой безопасности	Отсутствует	Есть (Online Safety Act)	Частично (в рамках общей защиты детей)
Цифровое образование	Нет обязательных программ	Обязательная программа во всех школах	С 1 класса, интеграция в предметы
Подготовка специалистов	Ограниченная	Специальные тренинги для учителей и полицейских	Обязательная подготовка педагогов и психологов
Взаимодействие ведомств	Фрагментарное	Координация через UKCIS	Школьные команды + местные органы
Реакция на угрозы	Чаще реактивная	Превентивная и системная	Превентивная и эмоционально-ориентированная

Изучение международного опыта свидетельствует, что для эффективной защиты прав ребёнка в цифровом пространстве необходимы как принятие нормативно-правовых актов, так и развитая система образования, профилактики и координация. Узбекистан обладает всеми возможностями для внедрения лучших мировых практик с учётом национальной специфики.

Подытоживая вышеотмеченные, можно прийти к выводу что, исходя из опыта Великобритании и Финляндии в Узбекистане необходимо:

- Разработать национальный правовой акт о цифровой безопасности детей, аналогичного *Online Safety Act*;
- Разработка и внедрение обязательного национального образовательного модуля по цифровой грамотности в школьные программы, начиная с начальной школы;
- Создание школьных команд цифровой поддержки, включающих педагогов, психологов и IT-специалистов, как в Финляндии;
- Обучение педагогов и школьных психологов по вопросам выявления и предотвращения онлайн-угроз;
- Формирование единого межведомственного координационного органа, ответственного за защиту детей в цифровом пространстве.

Исходя из этого, в условиях ускоренного развития цифровых технологий и растущей вовлечённости несовершеннолетних в онлайн-пространство, становится объективно необходимым формирование комплексной системы правового регулирования в сфере цифровой безопасности, ориентированной как на обеспечение защиты, так и на полноценное развитие правового статуса ребёнка в цифровой среде. Представленные в исследовании выводы и предложения, основанные на системном анализе национальной и международной практики (включая модели Великобритании и Финляндии), позволяют определить стратегические направления совершенствования законодательства и институционального устройства в Республике Узбекистан.

Имплементация предложенных мер – разработка и принятие специализированного нормативного акта, интеграция цифровой грамотности в образовательные программы, профессиональная подготовка профильных специалистов, формирование школьных команд цифровой поддержки, а также создание межведомственного координационного органа – будет способствовать не только усилению нормативно-правовой базы, но и формированию устойчивых компетенций цифровой безопасности у детей и взрослых.

Реализация этих инициатив позволит существенно повысить эффективность как превентивных, так и правоприменительных механизмов реагирования на цифровые риски, обеспечит целостную и системную защиту прав и законных интересов несовершеннолетних в информационно-коммуникационной среде, а также создаст правовые и институциональные условия для их безопасной социализации, самореализации и развития. Только за счёт сбалансированного взаимодействия правовых, образовательных и организационно-управленческих механизмов возможно построение эффективной и адаптированной к национальным реалиям модели цифровой защиты детей, соответствующей международным стандартам в области прав человека и прав ребёнка.

Сноски/ Иқтибослар/References:

1. Livingstone, S. (2018). *Children's digital rights and the boundaries of freedom online*. Journal of Digital Childhood Studies, 12(2), 45–61.
2. Kibby, M., & Helsper, E. (2020). *Balancing access and protection: Risks and opportunities in children's internet use*. Cyberpsychology Review, 15(3), 112–130.
3. Staksrud, E. (2017). *National regulation versus platform self-governance: Ensuring online safety for children*. International Review of Cyber Policy, 8(1), 27–43.
4. Gillespie, T. (2019). *Platform self-regulation and children's safety: Challenges and strategies*. Media & Society, 14(4), 98–115.
5. Конвенция о правах ребёнка от 20 ноября 1989 г. https://www.un.org/ru/documents/decl_conv/conventions/childcon.shtml
6. Комитет ООН по правам ребёнка. Общее замечание № 25 (2021): о правах ребёнка в цифровой среде // UNCRC General Comment No. 25 (2021).
7. Council of Europe. Strategy for the Rights of the Child (2022–2027) // <https://www.coe.int/en/web/children/strategy-2022-2027>.
8. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation, GDPR). Official Journal of the European Union, 2016. <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
9. Комитет по правам человека при ООН. Общие замечания № 25 о правах ребёнка в цифровой среде. 2021. https://www.refworld.org/ru/policy/concobservations/crc/2021/ru/146359?prevDestination=search&prevPath=/ru/search?ss_document_type_name%5B%5D=%D0%A0%D0%B5%D0%BA%D0%BE%D0%BC%D0%BC%D0%B5%D0%BD%D0%B4%D0%B0%D1%86%D0%B8%D0%B8+%D0%BF%D0%BE+%D0%B2%D0%BE%D0%BF%D1%80%D0%BE%D1%81%D0%B0%D0%BC+%D0%B4%D0%B8%D1%80%D0%B5%D0%BA%D1%82%D0%B8%D0%B2%D0%BD%D0%BE%D0%B3%D0%BE+%D1%85%D0%B0%D1%80%D0%B0%D0%BA%D1%82%D0%B5%D1%80%D0%B0&sort=score&order=desc&result=result-146359-ru
10. Конституция Республики Узбекистан от 30.04.2023 г. <https://lex.uz/docs/6445147>
11. Закон Республики Узбекистан «О гарантиях прав ребёнка» от 7 января 2008 г. <https://lex.uz/docs/1297318>
12. Закон Республики Узбекистан «О персональных данных» от 2 июля 2019 г.; <https://lex.uz/docs/4396428>
13. Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года (GDPR). <https://ogdpr.eu/ru/gdpr-2016-679>
14. Закон Республики Узбекистан «Об информатизации» от 11 декабря 2003 г.; <https://lex.uz/docs/82956>
15. Закон «О средствах массовой информации» от 26.12.1997 г. <https://lex.uz/docs/53112>
16. Конвенция Совета Европы о защите детей от сексуальной эксплуатации и сексуального насилия (Лансаротская конвенция). Ратифицирована Узбекистаном в 2021 г.
17. UNICEF Uzbekistan. Digital Literacy and Online Child Safety Report. Tashkent, 2023.
18. Бородин К.В. Проблемы правового регулирования безопасности в интернет-среде / К.В. Бородин // Вестник ЮУрГУ. Сер.: Право. – 2013. – Т. 13, № 3. – С. 104-105; Dubord P. Investigating Cybercrime / P. Dubord // Handbook of Digital and Multimedia Forensic Evidence / ed. J.J. Barbara. – Berlin: Springer, 2008. – P. 77-89.
19. Кучма В.Р. Охрана здоровья детей и подростков в Национальной стратегии действий в интересах детей на 2012– 2017 г. / В.Р. Кучма // Гигиена и санитария. – 2013. – № 6. – С. 26-30.

20. Проблемы обучения школьников безопасному использованию средств ИКТ / М.С. Анурьева, Н.Л. Королева, К.И. Остапчук [и др.] // Психолого-педагогический журнал «Гаудеамус». – 2017. – Т. 16, № 1. – С. 63-68.
21. Walden, K. (2020). *Legal frameworks for child protection in digital environments*. Journal of Internet Law and Policy, 14(3), 45-62.
22. Hoffman, L. (2021). *Why legal norms alone cannot ensure children's digital safety: The case for skills-based education*. Digital Pedagogy Review, 7(1), 112-130.
23. Abdullaeva, I. (2022). *Promoting safe online culture: The role of preventive digital education*. Journal of Educational Technology and Safety, 9(1), 33-49.
24. Martins, T. (2019). *Educational measures without legal backing: Limitations of awareness-only approaches to online child protection*. Educational Policy & Digital Rights, 5(2), 78-95.
25. UK Parliament. (2023). Online Safety Act. <https://www.legislation.gov.uk/ukpga/2023/50/enacted>
26. UK Council for Internet Safety. (2020). *Education for a Connected World Framework*. <https://www.gov.uk/government/publications/education-for-a-connected-world>
27. Finnish National Agency for Education. (2021). *National Core Curriculum for Basic Education*. <https://www.oph.fi/en/education-and-qualifications/national-core-curriculum-primary-and-lower-secondary-basic-education>
28. Mannerheim League for Child Welfare. <https://www.mll.fi/en/>

YURIST AXBOROTNOMASI

4-SON, 6-JILD

ВЕСТНИК ЮРИСТА

НОМЕР 4, ВЫПУСК 6

LAWYER HERALD

VOLUME 6, ISSUE 4

ISSN 2181-9416

DOI JURNAL: 10.26739/2181-9416