

УДК 342.7

КОНЦЕПЦИЯ КИБЕРБЕЗОПАСНОСТИ НЕСОВЕРШЕННОЛЕТНИХ КАК ОСНОВА РЕГУЛИРОВАНИЯ ВЗАИМОДЕЙСТВИЯ ДЕТЕЙ С ЦИФРОВОЙ СРЕДОЙ

Т. Н. Кузьменкова

старший преподаватель

Могилевский государственный университет имени А. А. Кулешова

аспирант

Белорусский государственный университет

В статье проводится анализ правового регулирования сферы взаимодействия несовершеннолетних с цифровой средой, акцентируется внимание на существующих угрозах. Исследуются способы обеспечения кибербезопасности несовершеннолетних, при этом анализируется опыт зарубежных стран. По итогам исследования предложены пути совершенствования национального законодательства в области кибербезопасности несовершеннолетних, в том числе обосновывается принятие Концепции кибербезопасности несовершеннолетних – документа, определяющего общие подходы, принципы, цели, задачи и механизм реализации государственной политики в сфере регулирования взаимодействия детей с киберпространством.

Ключавыя словы: дэструктыўнае інфармацыйнае ўздзеянне, інфармацыйная бяспекасць, кібербяспекасць несавершэнналетніх, кіберпрасторства, канцэпцыя.

Введение

Кибербезопасность несовершеннолетних как состояние их защищенности от кибератак, деструктивного информационного воздействия и правонарушений в киберпространстве является одной из наиболее актуальных с точки зрения необходимости совершенствования правового регулирования сфер.

Несмотря на достаточное количество нормативных правовых актов в сфере информационной безопасности и кибербезопасности в общем, анализ национального законодательства показывает, что сфера взаимодействия несовершеннолетних с киберпространством урегулирована не в полной мере, ряд вопросов находится вне правового поля, что может существенно в негативном контексте повлиять на права и законные интересы несовершеннолетних. В целом сфера кибербезопасности детей и подростков нуждается в комплексном правовом регулировании, основой которого должен стать единый документ, определяющий общие подходы, принципы, цели, задачи и механизм реализации государственной политики в сфере регулирования взаимодействия несовершеннолетних с киберпространством.

Данный документ станет продолжением вектора, заданного Конституцией, Концепцией информационной безопасности, Законом «О правах ребенка» и иными актами, а также выступит ориентиром в выработке конкретных мер по противодействию существующим в киберпространстве угрозам.

В этой связи цель настоящего исследования: определить направления совершенствования национального законодательства в сфере обеспечения кибербезопасности несовершеннолетних, в том числе в контексте разработки документа, закрепляющего общую стратегию по защите детей от информационных угроз и рисков в современной цифровой среде.

© Кузьменкова Т. Н., 2025

Основная часть

Активное обращение несовершеннолетних с информационными технологиями, в том числе в рамках учебного процесса, обуславливает необходимость обеспечения их безопасности в киберпространстве. Четкое правовое регулирование данной сферы будет способствовать максимальному снижению рисков нарушения прав детей и позволит защитить их от существующих угроз, к которым можно отнести: кибератаки, непосредственно направленные на технические средства, системы и технологии (например, использование вредоносных программ, несанкционированный доступ к компьютерной информации); негативное влияние компьютерных игр на психическое и физическое здоровье; деструктивное информационное воздействие на нравственную и мировоззренческую сферу, в том числе вовлечение в преступную и антигосударственную деятельность; совершение правонарушений и иных деяний, посягающих на права несовершеннолетних, с использованием киберпространства (интернет-мошенничество, кибербуллинг, онлайн-груминг); распространение информации о несовершеннолетних, которая в последующем может быть использована в ущерб их интересам.

Правовое регулирование защиты от существующих угроз информационной безопасности детей в киберпространстве базируется на Конституции Республики Беларусь, закрепившей наряду со свободой мнений, убеждений и их свободным выражением (ст.33) возможность ограничения прав и свобод в интересах национальной безопасности, общественного порядка, защиты нравственности, здоровья населения, прав и свобод других лиц (ст.23). Кроме того, последние изменения Основного Закона содержат ориентиры в отношении допустимой к распространению информации, что вытекает из норм об осуществлении демократии на основе идеологии белорусского государства (ст.4). Обновленный Основной Закон содержит нормы, касающиеся защиты персональных данных и безопасности личности и общества при их использовании [1].

Что касается непосредственно прав и свобод несовершеннолетних, стоит обратить внимание на статью 32¹ (государство способствует духовному, нравственному, интеллектуальному и физическому развитию молодежи), а также на обязанность родителей воспитывать детей, заботиться об их здоровье, развитии и обучении (ст.32) [1]. Продолжение заданного Конституцией вектора воспитания детей и молодежи нашло отражение в Концепции непрерывного воспитания детей и учащейся молодежи, утвержденной Постановлением Министерства образования Республики Беларусь 15 июля 2015 г. № 82; Стратегии развития государственной молодежной политики Республики Беларусь до 2030 года, утвержденной Постановлением Совета Министров Республики Беларусь 19 июня 2021 г. № 349.

Общие вопросы обеспечения информационной безопасности, как состояния защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере [2], и кибербезопасности как состояния защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз [3], регулируются Концепцией информационной безопасности Республики Беларусь, утвержденной Постановлением Совета Безопасности Республики Беларусь 18.03.2019 № 1, Указом Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности».

Более предметно вопросы информационной безопасности детей регулируются Законом Республики Беларусь № 2570-ХІІ от 19 ноября 1993 г. «О правах ребенка», с изменениями от 19 мая 2022 г. № 171-З (далее Закон), который в статье 37¹ закрепляет право детей на защиту от информации, причиняющей вред их здоровью и развитию и перечисляет разновидности информации, способной оказать негативное влияние на здоровье, физическое, нравственное и духовное развитие детей. В отношении распро-

страняемого контента в государстве устанавливается возрастная категоризация. Кроме того согласно ч.7 статьи 37² Закона в целях обеспечения защиты детей от информации, причиняющей вред их здоровью и развитию, распространяемой в глобальной компьютерной сети Интернет, собственники компьютерных клубов, интернет-кафе, иных мест, в которых обеспечивается коллективный доступ пользователей к глобальной компьютерной сети Интернет, учреждения образования обязаны применять административные, организационные меры, программно-аппаратные и программные средства, позволяющие не допустить распространения среди детей информации, причиняющей вред их здоровью и развитию [4].

Вместе с тем анализ национального законодательства показывает, что сфера взаимодействия несовершеннолетних с киберпространством регулируется частично, ряд вопросов находится вне правового поля, что может существенно в негативном контексте повлиять на права и законные интересы несовершеннолетних.

Непроработанными или недостаточно урегулированными в законодательстве остаются следующие вопросы:

- закрепление права несовершеннолетних на кибербезопасность;
- сфера ответственности родителей за обеспечение безопасности детей при их взаимодействии с киберпространством;
- механизм реализации несовершеннолетними права на защиту от информации, причиняющей вред их здоровью и развитию, распространяемой в информационно-коммуникационной сети «Интернет». В том числе отсутствует детальное правовое регулирование допустимости способов и приемов распространения информации, которое бы предусматривало защиту от различных вариантов манипулятивного информационного воздействия. Авторы научно-практического пособия «Фейковизация как средство информационной войны в интернет-медиа» к подобным способам и приемам относят: «Утаивание психологически важной информации или включение значимой информации в общий контекст информационного потока; намеренное упрощение и суггестия, выражающаяся в целенаправленном повторении; изменение смысла понятий...; намеренное включение широко известного образа – известных политических деятелей, представителей шоу-бизнеса...; ангажированность в освещении событий, акцентирование и поиск негатива в абсолютно любом явлении, происходящем в обществе; использование собственно «фейк-ньюс», создающих эмоциональную волну; вынесение абсурдной либо спорной мысли в заголовок в форме вопроса или предположения...» [5, с. 8].
- слабо урегулированной остается область компьютерных игр, как с точки зрения подаваемого контента, так и времени, проводимого ребенком за игрой;
- правонарушения против интересов несовершеннолетних, которые сопряжены с использованием киберпространства (прежде всего сексуальные домогательства в отношении детей в сети), по мнению ряда исследователей нуждаются в закреплении отдельными составами;
- недостаточно проработанной является защита несовершеннолетних от распространения о них информации в сети Интернет (фотографии, видеоролики), которая в последующем может причинить вред их правам и законным интересам.

Таким образом, правовое регулирование взаимодействия детей и подростков с киберпространством нуждается в совершенствовании.

Анализ опыта зарубежных государств по защите детей и подростков от угроз в цифровой среде показывает действенность следующих мер государственно-правового характера: категоризация контента, фильтрация контента, в том числе в рамках национального интернета (Исламская Республика Иран [6], Китайская Народная Республи-

ка [7]); авторизация пользователей, обязательная процедура подтверждения личности игроков в онлайн-видеоиграх; ограничение времени доступа к сети Интернет, в том числе запрет на доступ в ночное время; запрет на использование телефонов в учебных заведениях; услуга «родительский контроль»; криминализация отдельных деяний в сфере киберпространства, посягающих на права детей например, кибербуллинга, онлайн-груминга.

Одним из направлений противодействия деструктивному информационному воздействию на детей и подростков выступает принятие документов, комплексно регулирующих сферу взаимодействия несовершеннолетних с информацией с учетом общего информационного и ценностно-нравственного вектора развития государства, а также национальных интересов в различных сферах. Подобного рода документы выступают ориентиром для последующего правового регулирования сферы информационной безопасности несовершеннолетних.

В качестве примера можно привести Концепцию информационной безопасности детей в Российской Федерации (утверждена распоряжением Правительства Российской Федерации от 28 апреля 2023 г. № 1105-р), определившую общую стратегию по защите детей от информационных угроз и рисков в современной цифровой среде при условии эффективного сочетания государственных и общественных усилий при определяющей роли семьи. В числе направлений обеспечения информационной безопасности несовершеннолетних «Концепция предусматривает совершенствование механизмов выявления и пресечения распространения деструктивной информации; расширение практики межведомственного взаимодействия субъектов профилактики в предупреждении социально опасного поведения детей; развитие инфраструктуры, форм и методов первичной профилактики противоправного поведения подростков в сочетании с воспитательным воздействием в образовательных организациях; обеспечение защищенности персональных данных детей, размещенных в сети «Интернет», от публичного доступа и (или) их несанкционированного использования; расширение спектра возможностей услуги «Родительский контроль» на стационарных и мобильных устройствах, которыми пользуется ребенок; формирование у детей навыков самостоятельного и ответственного потребления информационной продукции; повышение грамотности детей по вопросам информационной безопасности» [8].

Помимо прочего Концепция устанавливает критерии оценки допустимости распространяемой информации, указывая, что она не должна противоречить традиционным российским духовно-нравственным ценностям, к которым в соответствии с Указом Президента Российской Федерации от 9 ноября 2022 г. № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» относятся жизнь, достоинство, права и свободы человека, патриотизм, гражданственность, служение Отечеству и ответственность за его судьбу, высокие нравственные идеалы, крепкая семья, созидательный труд, приоритет духовного над материальным, гуманизм, милосердие, справедливость, коллективизм, взаимопомощь и взаимоуважение, историческая память и преемственность поколений, единство народов России [9].

Совершенствование национального государственно-правового механизма регулирования взаимодействия несовершеннолетних с киберпространством, на наш взгляд, должно развиваться по нескольким направлениям.

Во-первых, максимальное использование возможностей технических и программных средств защиты, правовое регулирование их применения. Установление прямых ограничительных мер: запрет на доступ к определенным ресурсам, ограничение времени, проводимого в сети, в том числе в ночное время, авторизация для пользователей

сетевых компьютерных игр, с подтверждением возраста, локальный «Детский интернет» и другие.

Во-вторых, четкая фиксация субъектов, ответственных за безопасность несовершеннолетних в киберпространстве (родители и лица, их заменяющие, учреждения образования, владельцы заведений с доступом к сети и других) и области их ответственности.

В-третьих, определение зоны ответственности несовершеннолетних за свое поведение в сети, кибергигиена несовершеннолетних.

В-четвертых, совершенствование законодательства в сфере обеспечения кибербезопасности несовершеннолетних целесообразно вести и в направлении закрепления специальных составов противоправных деяний, посягающих на права, свободы и законные интересы несовершеннолетних, совершаемых с использованием киберпространства.

Однако для согласованного развития данных направлений, по мнению автора, необходим документ, закрепляющий общую стратегию по защите детей от информационных угроз и рисков в современной цифровой среде – Концепция кибербезопасности несовершеннолетних.

Концепция кибербезопасности несовершеннолетних как совокупность официальных взглядов на обеспечение безопасности несовершеннолетних в киберпространстве, станет документом, определяющим общие подходы, принципы, цели, задачи и механизм реализации государственной политики в сфере регулирования взаимодействия детей с киберпространством и тем самым выступит ориентиром в выработке конкретных мер по противодействию существующим в киберпространстве угрозам.

Целью предлагаемой концепции должно стать обеспечение комплексного подхода к правовому регулированию взаимодействия несовершеннолетних с киберпространством.

Задачи концепции:

- анализ актуальных вызовов и угроз информационной безопасности детей и подростков в киберпространстве, определение направлений их нейтрализации;
- установление критериев деструктивного информационного воздействия на несовершеннолетних в киберпространстве;
- фиксация субъектов, вовлеченных в процесс обеспечения кибербезопасности детей, в том числе родителей и лиц, их заменяющих, а также зоны их ответственности;
- определение направлений совершенствования государственного механизма выявления и пресечения распространения деструктивной информации;
- формулировка приоритетных направлений эволюции правового регулирования сферы кибербезопасности несовершеннолетних;
- определение способов повышения уровня цифровой грамотности детей и подростков.

Структура предлагаемой концепции:

- отражение понятия, цели, задач, основных начал (принципов) и субъектов обеспечения кибербезопасности несовершеннолетних;
- закрепление критериев определения и видов деструктивного информационного воздействия на детей и подростков в киберпространстве, в том числе с учетом уже принятых актов в сфере государственной политики и безопасности;
- анализ современного состояния защиты детей в киберпространстве, выявление проблемного поля – и пробелов в правовом регулировании;
- определение приоритетных направлений совершенствования законодательства;
- прогнозирование ожидаемых результатов реализации Концепции.

По мнению автора, результатами **реализации Концепции** кибербезопасности несовершеннолетних в долгосрочной перспективе станут:

- создание национального государственно-правового механизма защиты несовершеннолетних от деструктивного информационного воздействия в цифровой среде;
- снижение рисков вовлеченности детей и подростков в деструктивные сообщества, осуществляющие свою деятельность с использованием сети «Интернет»;
- предупреждение и пресечение киберпреступлений и иных негативных деяний (например, кибербуллинга) в отношении несовершеннолетних;
- повышение уровня цифровой грамотности детей и подростков;
- вовлеченность родителей или лиц, их заменяющих в сфере обеспечения кибербезопасности несовершеннолетних в рамках исполнения ими конституционной обязанности по воспитанию детей;
- сокращение в сети «Интернет» контента деструктивного характера и, напротив, увеличение в сети контента, соответствующего традиционным ценностным ориентирам белорусского народа, и в целом направлений обеспечения национальной безопасности государства.

На основе Концепции кибербезопасности несовершеннолетних с учетом закрепленных в ней критериев определения деструктивного информационного воздействия в киберпространстве, а также субъектов, ответственных за обеспечение кибербезопасности детей и подростков и направлений эволюции национального законодательства можно будет детально совершенствовать правовое регулирование следующих сфер:

- организационно-правовой механизм контроля потребляемого несовершеннолетними контента в сети «Интернет» и времени, проводимого в сети;
- сетевые компьютерные игры;
- личная информация, хранящаяся, накапливаемая и распространяемая в киберпространстве;
- сфера противоправных деяний в киберпространстве;
- сфера родительской ответственности по обеспечению кибербезопасности детей и подростков.

Таким образом, разработка базового документа, регулирующего область информационной безопасности несовершеннолетних в киберпространстве, станет стимулом и ориентиром принятия последующих организационно-правовых решений.

Заключение

Эволюция социума в информационное общество обуславливает актуальность сферы кибербезопасности личности. Особенно детально данная область общественных отношений должна быть проработана в отношении детей и подростков.

Взаимодействия несовершеннолетних с цифровой средой подлежит правовому регулированию прежде всего в части допустимости потребляемого контента, а также определения вариаций деструктивного информационного воздействия в киберпространстве, и должно осуществляться с учетом вызовов и угроз современности, принятых актов в сфере государственной политики и безопасности.

Основой правового регулирования взаимодействия детей с цифровой средой может стать Концепция кибербезопасности несовершеннолетних, в которой следует отразить критерии определения деструктивного информационного воздействия на несовершеннолетних; дать характеристику актуальных вызовов и угроз, выделить основные направления их нейтрализации; определить круг субъектов, вовлеченных в процесс обеспечения кибербезопасности детей, а также зону их ответственности; закрепить приоритетные направления эволюции правового регулирования сферы кибербезопасности несовершеннолетних.

Комплексный подход к правовому регулированию взаимодействия несовершеннолетних с киберпространством, обеспечиваемый Концепцией, позволит усовершенствовать на ее основе правовое регулирование иных вопросов, связанных с кибербезопасностью детей, в том числе в отношении механизма контроля потребляемого несовершеннолетними контента в сети «Интернет», времени, проводимого ими в сети; сферы сетевых компьютерных игр; сферы киберпреступлений и иных сфер.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Конституция Республики Беларусь [Электронный ресурс] : с изм. и доп., принятыми на респ. референдумах 24 нояб. 1996 г., 17 окт. 2004 г., 27 февр. 2022 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.
2. Концепция информационной безопасности Республики Беларусь [Электронный ресурс]: Утверждено Постановлением Совета Безопасности Республики Беларусь 18.03.2019 № 1. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.
3. О кибербезопасности [Электронный ресурс]: Указ Президента Республики Беларусь, 14 февраля 2023 г., № 40 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.
4. О правах ребенка [Электронный ресурс]: Закон Респ. Беларусь от 19 ноября 1993 г. № 2570-ХІІ : в ред. Закона Респ. Беларусь от 19.05.2022 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.
5. Фейковизация как средство информационной войны в интернет-медиа : научно-практическое пособие. – Москва : Блок-Принт, 2023. – 144 с.
6. Ковалев, О. Г. Кибербезопасность в условиях национального Интернета (Иранский опыт противодействия киберугрозам) [Электронный ресурс] / О. Г. Ковалев, А. А. Скипидаров // Столыпинский вестник. – 2021. – Режим доступа: <https://cyberleninka.ru/article/n/kiberbezopasnost-v-usloviyah-natsionalnogo-interneta-iranskiy-opyt-protivodeystviya-kiberugrozam/viewer>. – Дата доступа: 01.07.2024.
7. Горян, Э. В. Нормативно-правовая основа обеспечения национальной безопасности в киберпространстве: опыт Китайской Народной Республики [Электронный ресурс] / Э. В. Горян // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. – 2021. – №1. – Режим доступа: <https://cyberleninka.ru/article/n/normativno-pravovaya-osnova-obespecheniya-natsionalnoy-bezopasnosti-v-kiberprostranstve-opyt-kitayskoy-narodnoy-respubliki/viewer>. – Дата доступа: 01.07.2024.
8. Концепция информационной безопасности детей в Российской Федерации [Электронный ресурс]. – Режим доступа: <https://www.vedomosti.ru/society/articles/2023/05/10/974297-pravitelstvo-utverdilo-kontseptsiyu-informatsionnoi-bezopasnosti-detei> – Дата доступа: 09.07.2024.
9. Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей [Электронный ресурс] Указ Президента Российской Федерации от 09.11.2022 № 809 Режим доступа: <https://www.garant.ru/products/ipo/prime/doc/405579061/>. – Дата доступа: 14.07.2024.

Поступила в редакцию 13.10.2024 г.

Контакты: kuzmenkova@m.msu.by (Кузьменкова Татьяна Николаевна)

Kuzmenkova T. N. CONCEPT OF CYBERSECURITY FOR MINORS AS A FOUNDATION FOR REGULATING CHILDREN'S INTERACTION WITH THE DIGITAL ENVIRONMENT

The article analyzes the legal regulation governing the interaction of minors within the digital environment, emphasizing existing threats. It investigates methods for ensuring the cybersecurity of minors, examining international practices. Based on the results of the study, the author proposes ways to enhance national legislation concerning the cybersecurity of minors, including a rationale for adopting a Concept of Cybersecurity for Minors – a document defining general approaches, principles, goals, objectives, and mechanisms for implementing state policy in regulating children's interaction with cyberspace.

Keywords: destructive information impact, information security, cybersecurity of minors, cyberspace, concept