

МРНТИ 10.81.71
УДК 342
JEL K14

<https://doi.org/10.46914/2959-4197-2026-1-3-272-284>

ХАСАНОВА В.В.,*¹

М.Ю.Н.

*e-mail: vikakiper85@bk.ru

ORCID ID: 0000-0001-5579-1565

БЕГИМБАЕВ С.А.,²

к.ю.н., ст. преподаватель.

e-mail: begimbaev.serik@mail.ru

ORCID ID: 0009-0008-1383-9223

¹Актюбинский юридический институт

МВД Республики Казахстан им. М. Букембаева,

г. Актюбе, Казахстан

²Алматинский гуманитарно-экономический

университет,

г. Алматы, Казахстан

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НЕСОВЕРШЕННОЛЕТНИХ: МЕЖДУНАРОДНЫЕ АКТЫ И СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА ЗАРУБЕЖНЫХ СТРАН

Аннотация

В статье исследуется формирование многоуровневой системы международно-правовой и национальной защиты несовершеннолетних от информационных угроз в цифровой среде. Актуальность обусловлена тем, что цифровые коммуникации стали самостоятельным пространством социализации детей и подростков, а риски часто реализуются в скрытой коммуникационной форме (кибербуллинг, онлайн-груминг, распространение деструктивного и сексуализированного контента, неправомерное использование персональных данных), что затрудняет раннее выявление и правовую оценку. Целью исследования является выявление ключевых международных стандартов и сопоставление регуляторных и уголовно-правовых моделей реагирования, формируемых в различных юрисдикциях. Методологическая база включает формально-юридический и герменевтический анализ международных и национальных актов, системный и структурно-функциональный подходы к оценке распределения обязанностей государства и цифровых посредников, а также сравнительно-правовой метод для выявления общих тенденций и различий (включая стандарты Совета Европы по киберпреступности и защите детей от сексуальной эксплуатации). Показано, что современная модель защиты все в большей степени смещается от исключительно уголовного преследования к сочетанию криминализации и превентивного регулирования платформ.

Ключевые слова: информационная безопасность несовершеннолетних, цифровая среда, киберугрозы, онлайн-груминг, кибербуллинг, персональные данные детей, международные стандарты.

Введение

Стремительная цифровизация общественных отношений и расширение глобального информационного пространства обусловили появление новых угроз для несовершеннолетних как наиболее уязвимой категории пользователей. Цифровая среда уже не ограничивается функцией вспомогательного канала связи и обучения, а выступает самостоятельным пространством социализации, в котором формируются модели поведения, ценностные установки и коммуникативные практики детей и подростков. Уязвимость несовершеннолетних определяется не только возрастными психологическими особенностями, но и недостаточным знанием рисков цифровой среды, а также ограниченными возможностями самостоятельной правовой и технической защиты от противоправного воздействия.

По данным Международного союза электросвязи, около 77 процентов молодых людей в возрасте от 15 до 24 лет активно пользуются Интернетом [1]. Это создает широкие возможнос-

ти для образования, общения и участия в общественной жизни, но одновременно порождает серьезные риски, включая кибербуллинг, онлайн-груминг, распространение деструктивного и сексуализированного контента, неправомерное использование персональных данных и манипулятивное воздействие на ребенка. Дополнительную сложность создает то, что такие угрозы часто реализуются в скрытой форме и маскируются под обычное общение, развлекательный либо образовательный контент, что затрудняет их своевременное выявление, фиксацию и правовую оценку.

Осознание масштабов этих рисков привело к формированию многоуровневой системы международно-правовой защиты детей в цифровой среде. Она включает международные договоры, акты «мягкого права», политические декларации, директивы, руководящие принципы и национальные нормативные модели, закрепляющие необходимость сочетания правовых, организационных, технологических и образовательных мер при безусловном приоритете наилучших интересов ребенка. Одновременно государства адаптируют национальное уголовное законодательство к цифровой среде, расширяя перечень наказуемых деяний, уточняя составы преступлений, совершаемых с использованием информационно-коммуникационных технологий, и возлагая дополнительные обязанности на цифровые платформы как ключевых посредников современного информационного обмена.

Объектом настоящего исследования выступают общественные отношения, складывающиеся в сфере международно-правовой и национальной защиты несовершеннолетних от информационных угроз в цифровой среде.

Предмет исследования составляют международные акты, зарубежные уголовно-правовые и регуляторные модели, а также отдельные положения законодательства Республики Казахстан, направленные на предупреждение, выявление и пресечение посягательств на информационную безопасность несовершеннолетних.

Цель исследования заключается в выявлении основных международных стандартов защиты несовершеннолетних в цифровой среде и проведении сравнительно-правового анализа уголовного законодательства зарубежных стран в части противодействия информационным угрозам, затрагивающим права, свободы и законные интересы детей.

Достижение указанной цели предполагает решение следующих задач: раскрыть содержание международно-правовых стандартов защиты прав ребенка в цифровой среде; определить значение Конвенции о правах ребенка, Замечания общего порядка № 25 Комитета ООН по правам ребенка, Будапештской и Лансаротской конвенций для формирования современных подходов к защите несовершеннолетних; проанализировать уголовно-правовые и регуляторные механизмы, используемые в отдельных зарубежных государствах; выявить общие тенденции криминализации деяний, связанных с онлайн-грумингом, сексуальной эксплуатацией, кибербуллингом, незаконным оборотом материалов сексуального насилия над детьми и неправомерным использованием персональных данных; определить возможности использования зарубежного опыта при дальнейшем совершенствовании законодательства Республики Казахстан.

Практическая значимость исследования состоит в том, что сформулированные выводы и предложения могут быть использованы при совершенствовании национального законодательства в сфере защиты детей от вредной информации, развитии уголовно-правовых механизмов противодействия цифровым угрозам, подготовке методических рекомендаций для правоохранительных органов, а также при разработке профилактических мер, направленных на повышение цифровой безопасности несовершеннолетних.

Особое значение результаты исследования имеют для обоснования необходимости комплексного подхода, при котором уголовно-правовое реагирование сочетается с превентивным регулированием цифровых платформ, защитой персональных данных детей, возрастн-ориентированным проектированием цифровых сервисов и международным сотрудничеством в расследовании трансграничных киберпреступлений.

В совокупности это формирует научную и прикладную основу для оценки современных моделей защиты несовершеннолетних в цифровой среде и определения направлений дальнейшей адаптации законодательства к новым технологическим, криминологическим и правоприменительным вызовам.

Материалы и методы

Эмпирико-документальную базу исследования (материалы) образовали международные договоры и акты «мягкого права» в сфере прав ребенка и кибербезопасности, акты наднационального регулирования, национальные законы и подзаконные документы отдельных государств, а также официальные руководящие принципы регуляторов и обобщаемые сведения из международных докладов и отчетов, используемые в работе как вторичные данные для характеристики масштабов и типологии угроз. Дополнительно учитывались отдельные судебные позиции и правоприменительные ориентиры, значимые для оценки допустимых пределов вмешательства и выбора правовых средств (в той мере, в какой они отражают закрепленные подходы к защите несовершеннолетних в цифровой среде).

Методологическую основу исследования составил комплекс взаимодополняющих общенаучных и специальных юридических методов, выбор которых обусловлен межуровневой природой объекта и необходимостью сопоставления различных моделей регулирования. К ним относятся: диалектический метод, системный подход, структурно-функциональный анализ, нормативно-догматический (формально-юридический) метод, метод юридического толкования (герменевтический), сравнительно-правовой метод, логико-аналитические методы (анализ, синтез, индукция, дедукция), метод классификации и типологизации, документальный анализ и контент-анализ.

Совокупность указанных методов обеспечила корректное выявление и описание международных стандартов и национальных моделей защиты несовершеннолетних в цифровой среде как единого многоуровневого комплекса и обоснованное сопоставление правовых решений, позволяющее оценивать направления дальнейшей адаптации законодательства к цифровым угрозам.

Результаты и обсуждение

Формирование системы международно-правовой защиты несовершеннолетних от информационных угроз не может быть понято вне контекста глобальной эволюции международной защиты прав человека. Фундаментальным документом, заложившим основу для защиты интересов детей в информационной сфере, является Конвенция Организации Объединенных Наций о правах ребенка, принятая резолюцией Генеральной Ассамблеи ООН 20 ноября 1989 г. [2]. Конвенция, ратифицированная практически всеми государствами – членами ООН, установила универсальную систему прав ребенка, ряд положений которой имеет прямое отношение к информационной безопасности. Статья 16 закрепляет право ребенка на защиту от произвольного или незаконного вмешательства в его личную жизнь, семейную жизнь, неприкосновенность жилища или тайну корреспонденции, а также от незаконных посягательств на его честь и репутацию. Статья 17, в свою очередь, обязывает государства-участников обеспечивать доступ детей к информации и материалам из различных национальных и международных источников, одновременно содействуя разработке надлежащих мер по защите ребенка от информации и материалов, наносящих вред его благополучию. Статья 34 устанавливает обязательства государства по защите ребенка от всех форм сексуальной эксплуатации и сексуального насилия, включая использование детей в порнографических изображениях и материалах. Эти нормы были приняты задолго до массового распространения Интернета, однако их формулировки оказались достаточно широкими для применения к угрозам современной цифровой эпохи.

Конкретизация обязательств государств в отношении противодействия сексуальной эксплуатации несовершеннолетних в цифровой среде была осуществлена Факультативным протоколом к Конвенции о правах ребенка, касающимся торговли детьми, детской проституции и детской порнографии, принятым в 2000 г. [2]. Протокол обязал государства криминализировать производство, распространение, импорт, экспорт, предложение, продажу или хранение детской порнографии, определяя ее как любое изображение ребенка, совершающего реальные или смоделированные откровенно сексуальные действия, либо любое изображение половых органов ребенка в сексуальных целях. Значимость протокола состоит в том, что он впервые на международном уровне закрепил обязанность государств преследовать данные деяния независимо от

технических средств их совершения, что позволило распространить соответствующие запреты на правонарушения, совершаемые с использованием информационно-коммуникационных технологий.

Качественно новый этап в развитии международно-правовых стандартов защиты несовершеннолетних в цифровом пространстве ознаменовало принятие Комитетом ООН по правам ребенка в 2021 г. Замечания общего порядка № 25 о правах детей в цифровой среде [3]. Указанный документ стал первым авторитетным толкованием положений Конвенции применительно к цифровому контексту и установил, что цифровая среда является не обособленной сферой правового регулирования, а представляет собой пространство, в котором все права ребенка, закрепленные Конвенцией, получают новое содержание и формы реализации. Замечание охватывает широкий спектр вопросов: защиту персональных данных детей, безопасность в онлайн-среде, защиту от экономической эксплуатации, свободу выражения мнения при одновременной защите от вредного контента, а также обязанности бизнес-структур в отношении влияния своей деятельности на права ребенка. Как отмечает С. Ливингстон, профессор Лондонской школы экономики и политических наук, данное Замечание является важным документом, требующим целостного обеспечения баланса прав на защиту, обеспечение и участие с учетом возраста и зрелости ребенка [4, с. 2]. Комитет обращает внимание на то, что развитие цифровых технологий оказывает существенное воздействие на права ребенка, однако практические механизмы оценки такого воздействия остаются ограниченными, а комплексный подход к правам детей, охватывающий не только право на защиту, но и права на обеспечение и участие, реализуется не в полной мере.

Существенную роль в международной защите несовершеннолетних в цифровой среде играет инициатива Международного союза электросвязи по защите детей в Интернете, чьи обновленные в 2020 г. руководящие принципы адресованы детям, родителям и педагогам, представителям индустрии и субъектам государственной политики. Дополнительное значение имеют типовые подходы Управления ООН по наркотикам и преступности и инструментарий МСЭ, ориентированные на согласование национальных и региональных мер противодействия цифровым угрозам. Их значимость обусловлена тем, что различия в уровне правоприменения и технической готовности государств требуют международного сотрудничества и укрепления институциональных возможностей для обеспечения равной защиты детей независимо от страны проживания.

На следующем уровне ключевую роль в формировании правовых стандартов противодействия киберпреступности играет Будапештская конвенция о киберпреступности, принятая Советом Европы 23 ноября 2001 г. Она стала первым международным договором, непосредственно направленным на гармонизацию уголовного законодательства государств в сфере противодействия правонарушениям в информационном пространстве [5].

Конвенция устанавливает обязательства государств-участников по криминализации несанкционированного доступа к компьютерным системам, незаконного перехвата данных, вмешательства в функционирование информационных систем, а также правонарушений, связанных с детской порнографией. Статья 9 требует криминализации производства, предложения, распространения, передачи, приобретения и хранения детской порнографии с использованием компьютерных систем, определяя при этом понятие детской порнографии достаточно широко для охвата как изображений, так и реалистичных образов несовершеннолетних, вовлеченных в откровенно сексуальное поведение. Как подчеркивает С. Бреннер, принятие специальных норм о киберпреступности является шагом к признанию того, что киберпреступления представляют собой новый феномен и форму глобализации преступного поведения; если развитые государства не примут согласованного законодательства, они лишатся морального основания критиковать другие страны за неспособность сделать то же самое [6, с. 14].

Вместе с тем практическая эффективность Будапештской конвенции зависит от ряда факторов. Из числа подписантов лишь часть государств своевременно ратифицировала документ; ряд крупных государств, включая Российскую Федерацию и Китайскую Народную Республику, не присоединились к Конвенции, ссылаясь на вопросы суверенитета и трансграничного доступа к данным. Более того, стремительное развитие технологий, включая появление криптографических инструментов, анонимных сетей, облачных хранилищ и криптовалют, создает вызовы, которые не были предусмотрены разработчиками документа на рубеже тысячелетий.

Лансаротская конвенция Совета Европы о защите детей от сексуальной эксплуатации и сексуального насилия, принятая в 2007 г., стала первым международным документом, квалифицирующим различные формы сексуального насилия над детьми как уголовные преступления, включая деяния, осуществляемые с использованием информационно-коммуникационных технологий [7]. Конвенция предусматривает криминализацию онлайн-груминга, то есть создания доверительного контакта с ребенком с целью сексуальной эксплуатации, производство и распространение материалов сексуального насилия над детьми, а также устанавливает превентивные меры, включающие проверку и обучение лиц, работающих с детьми, и информирование самих несовершеннолетних о рисках. Глобальный альянс WeProtect рассматривает ратификацию Лансаротской конвенции в качестве ключевого ориентира для государств на пути к согласованию законодательства, подчеркивая необходимость глобальной гармонизации регуляторных режимов для предотвращения использования правонарушителями правовых лакун между юрисдикциями. Мы придерживаемся позиции, согласно которой значение Лансаротской конвенции выходит за рамки криминализации отдельных деяний и заключается в закреплении комплексного подхода, сочетающего уголовно-правовые, превентивные и реабилитационные меры. Именно этот подход стал модельным для современного национального законодательства и прослеживается в реформах уголовного права Германии, Франции, Великобритании и других государств, о которых речь пойдет дальше.

В рамках Европейского Союза ключевое значение для защиты несовершеннолетних в цифровой среде приобрел Акт о цифровых услугах, вступивший в силу в августе 2023 г. для очень крупных онлайн-платформ и с февраля 2024 г. – для остальных платформ [8]. Статья 28 Акта устанавливает обязанность онлайн-платформ, доступных несовершеннолетним, принимать надлежащие и соразмерные меры для обеспечения высокого уровня конфиденциальности, безопасности и защищенности несовершеннолетних; при этом запрещается таргетированная реклама, основанная на профилировании персональных данных детей.

В июле 2025 г. Европейская комиссия опубликовала руководящие принципы защиты несовершеннолетних в рамках настоящего Акта, содержащие рекомендации по установке приватных аккаунтов по умолчанию, внедрению верификации возраста и защите от манипулятивной коммерческой практики. Регуляторная модель Европейского Союза отличается тем, что возлагает ответственность на технологические платформы, устанавливая санкции до шести процентов глобального оборота за несоблюдение требований. Подобный подход отражает осознание того факта, что эффективная защита несовершеннолетних в цифровой среде невозможна только средствами традиционного уголовного преследования, она требует системного регулирования деятельности посредников, через которых осуществляется доступ к информационному пространству.

Обращаясь к анализу уголовного законодательства зарубежных государств, необходимо прежде всего обратить внимание на правовую систему Соединенных Штатов Америки, где сложилась многоуровневая модель регулирования, сочетающая федеральное законодательство и законодательство штатов. Базовым федеральным актом в сфере защиты цифровых данных несовершеннолетних является закон о защите конфиденциальности детей в Интернете 1998 г., обязывающий операторов веб-сайтов и онлайн-сервисов, сознательно собирающих персональные данные детей в возрасте до тринадцати лет, получать верифицированное согласие родителей [9].

В сфере уголовного права центральное значение имеют параграфы 2251, 2252 и 2252А Раздела 18 Свода законов США, устанавливающие уголовную ответственность за производство, транспортировку, распространение и хранение материалов, содержащих изображения сексуальных действий с участием несовершеннолетних, с санкциями, достигающими тридцати лет лишения свободы [9]. Как справедливо отмечает С. Бреннер, соотношение федерального законодательства и законодательства штатов в сфере киберпреступности порождает вариативность и неоднозначность, поскольку законодатели штатов сталкиваются с дилеммой: с одной стороны, перед ними, казалось бы, совершенно новые виды преступной деятельности, требующие принятия нового материального уголовного законодательства, с другой – можно утверждать, что речь идет лишь о традиционных деяниях, совершаемых новыми способами [6, с. 28]. Данная дилемма имеет не только теоретическое, но и практическое значение, поскольку определяет

подход к квалификации деяний и выбору применимых правовых норм. В основе лежит то, что именно федеральная модель, при которой специализированные нормы о киберпреступлениях не подменяют общие уголовно-правовые нормы, демонстрирует наибольшую эффективность в условиях стремительного развития технологий.

Существенный интерес представляет судебная практика Верховного суда США, который в 2024 г. подтвердил конституционность закона штата Техас, требующего проверки возраста для доступа к контенту, предназначенному для взрослых. Настоящее решение, имеющее прецедентное значение, способно повлиять на законодательные инициативы как на уровне штатов, так и на федеральном уровне. Проблема проверки возраста является одной из наиболее дискуссионных в современном информационном праве, поскольку технические методы ее осуществления неизбежно затрагивают право на конфиденциальность и анонимность, в том числе несовершеннолетних. Допустимо предположить, что баланс между эффективностью верификации и защитой персональных данных будет определяться не столько правовыми нормами, сколько технологическими решениями, позволяющими подтвердить возраст без раскрытия избыточной информации о личности пользователя.

В этой связи внимание уделяется опыту Франции, где регулятор ARCOM в 2025 г. установил технические стандарты проверки возраста для порнографических сайтов, ряд которых предпочел блокировать доступ с территории Франции вместо соблюдения требований.

Великобритания сформировала одну из наиболее развитых систем регулирования информационной безопасности несовершеннолетних. Закон об онлайн-безопасности 2023 г. возлагает на поставщиков интернет-услуг обязательства по защите несовершеннолетних пользователей от вредного контента, закрепляет обязанность проявлять должную заботу и наделяет регулятора Ofcom полномочиями по контролю за исполнением этих требований [10].

Кодекс возрастного проектирования 2021 г., разработанный Управлением комиссара по информации, содержит пятнадцать основанных на положениях Конвенции ООН о правах ребенка стандартов проектирования цифровых услуг с учетом интересов детей. Настоящий Кодекс стал образцом соответствующего законодательства в других юрисдикциях, включая штат Калифорния в США. Уголовное преследование киберпреступлений в Великобритании осуществляется на основании закона о неправомерном использовании компьютеров 1990 г.; Королевская прокурорская служба в своих руководящих разъяснениях различает киберзависимые преступления, возможные исключительно при использовании информационно-коммуникационных технологий, и киберобусловленные традиционные правонарушения, масштабируемые с помощью цифровых технологий. Оба вида в определенной степени затрагивают интересы несовершеннолетних. Мы исходим из того, что британская модель характеризуется системностью и многоуровневостью: она сочетает уголовно-правовые механизмы с регуляторным воздействием на платформы и стандартами проектирования, которые создают комплексную архитектуру защиты, не сводимую к одному лишь карательному механизму.

Уголовное законодательство Федеративной Республики Германия отличается детальной регламентацией ответственности за посягательство на информационную безопасность несовершеннолетних. Уголовный кодекс ФРГ криминализует распространение порнографических материалов с участием несовершеннолетних (пункт 184), распространение материалов сексуального насилия над детьми (пункт 184b) и кибергroomинг (пункт 176a) [11].

В 2021 г. германский законодатель осуществил принципиальную реформу, переведя распространение материалов сексуального насилия над детьми из категории менее тяжких деяний в разряд преступлений с минимальным наказанием в виде одного года лишения свободы. Данное решение непосредственно связано с ужесточением уголовной ответственности за деяния, посягающие на информационную безопасность несовершеннолетних, и свидетельствует о признании законодателем их повышенной общественной опасности, несмотря на существующую дискуссию о пределах криминализации. Закон о защите молодежи, реформированный в том же 2021 г., расширил требования к цифровым платформам, обязав их внедрять механизмы верификации и обеспечения безопасности по умолчанию. Германский подход примечателен тем, что он сочетает традиционное уголовно-правовое регулирование, характерное для континентальной системы, с элементами регуляторного воздействия на процессы цифровых компаний, заимствованными из англосаксонской практики.

Французская Республика в настоящее время занимает одну из лидирующих позиций по строгому регулированию доступа несовершеннолетних к контенту для взрослых. Закон № 2024-449 о верификации возраста обязывает операторов веб-сайтов, содержащих такой контент, внедрять надежные средства подтверждения возраста пользователей.

Уголовный кодекс Франции криминализирует вовлечение несовершеннолетних в порнографию (статьи 227-22 и 227-23); статья 227-22-1, введенная в 2020 г., устанавливает уголовную ответственность за онлайн-груминг, то есть действия по установлению контакта с несовершеннолетним с помощью электронных коммуникаций с целью совершения в отношении него сексуального преступления или правонарушения. Французский опыт свидетельствует о готовности законодателя к принятию жестких мер, однако одновременно выявляет практические трудности их реализации: часть платформ блокирует доступ из соответствующей юрисдикции вместо выполнения требований о верификации возраста, что ставит вопрос об эффективности такой меры в условиях трансграничного характера цифрового пространства.

Китайская Народная Республика реализует один из наиболее всеобъемлющих подходов к регулированию информационной безопасности несовершеннолетних. Закон о защите несовершеннолетних, пересмотренный в 2020 г., включает отдельную главу о защите в сетевом пространстве, устанавливающую обязательную регистрацию под реальным именем и ограничение игрового времени несовершеннолетних в течение недели. Закон о защите персональных данных 2021 г. требует получения согласия на обработку данных от лиц, не достигших четырнадцатилетнего возраста.

Китайская модель отличается высокой степенью государственного контроля над информационным пространством, что обеспечивает значительные возможности для ограничения доступа несовершеннолетних к вредному контенту, но одновременно вызывает вопросы соразмерности и совместимости с правами ребенка на доступ к информации и свободу выражения мнений. По нашему убеждению, оценка эффективности таких моделей должна учитывать специфику политической и законодательной системы государства, что затрудняет прямое заимствование ее элементов в других правовых контекстах.

Австралия предприняла одну из наиболее радикальных мер в мировой практике – законодательный запрет на использование социальных сетей детьми в возрасте до шестнадцати лет, вступающий в силу в декабре 2025 г. Такое решение вызвало международную дискуссию. Как считает С. Ливингстон, исследовавшая практику запретительных мер, одни лишь ограничения и запреты не дают устойчивого результата. Необходим системный подход, включающий переосмысление и редизайн технологий с учетом прав и интересов детей [4, с. 7]. Указанная позиция отражает более широкую дискуссию о пределах государственного запрета в информационном пространстве: если запретительные меры без разумного технологического обеспечения легко обходятся несовершеннолетними, их декларативный характер может подрывать доверие к системе защиты.

С другой стороны, установление четкого возрастного порога создает правовую определенность и возлагает на платформы юридически обязывающее требование, невыполнение которого влечет ответственность. Можно утверждать, что оптимальная модель должна сочетать элементы возрастных ограничений с требованиями к дизайну и функциональности цифровых платформ, обеспечивающими безопасность по умолчанию.

Сравнительно-правовой анализ различных юрисдикций позволяет выявить ряд устойчивых изменений в развитии уголовно-правовой охраны информационной безопасности несовершеннолетних. Прежде всего наблюдается постепенное расширение перечня криминализируемых деяний: от традиционного противодействия производству и распространению детской порнографии – к криминализации онлайн-груминга, кибербуллинга, несанкционированного сбора данных детей и манипулятивного дизайна цифровых услуг. Данная тенденция отражает эволюцию представлений законодателя о характере угроз: если на начальном этапе основное внимание уделялось контентным рискам, то в настоящее время осознается необходимость противодействия коммуникативным и поведенческим рискам, возникающим при использовании цифровых платформ.

Прослеживается также ужесточение санкций. К примеру, Германия перевела распространение материалов сексуального насилия над детьми в категорию преступлений с более строгими

последствиями, а в США санкции за производство детской порнографии достигают тридцати лет лишения свободы. Формируется модель регуляторного давления на платформы, при которой ответственность за принятие мер по защите несовершеннолетних несут не только непосредственные правонарушители, но и посредники – прежде всего компании, обеспечивающие функционирование информационного пространства.

Классификация киберрисков для несовершеннолетних, разработанная в современной доктрине, позволяет систематизировать угрозы и определить приоритеты правового регулирования. Согласно исследованиям С. Ливингстон и ее коллег, киберриски подразделяются на контентные, связанные со столкновением с вредным содержанием, порнографией, пропагандой насилия и суицидальным контентом; коммуникационные, включающие кибербуллинг, онлайн-груминг и сексуальные домогательства; а также потребительские, связанные с мошенничеством, нарушением прав потребителей и манипулятивным маркетингом [4, с. 3]. Данная классификация имеет практическое значение для дифференциации правовых инструментов: контентные риски требуют модерации и возрастной маркировки, коммуникативные – криминализации отдельных форм поведения и развития способов обращения с жертвами, потребительские – развития регуляторных стандартов и контроля за бизнес-практиками. Представляется обоснованным утверждение, что эффективная правовая политика в данной сфере должна охватывать все три категории риска, а не концентрироваться исключительно на наиболее очевидных содержательных угрозах.

Сквозное шифрование остается одной из наиболее сложных дилемм в сфере информационной безопасности несовершеннолетних, поскольку, с одной стороны, оно защищает конфиденциальность коммуникаций, а с другой – затрудняет выявление противоправного контента и расследование преступлений против детей. Международные стандарты и практика зарубежных государств показывают, что эффективная защита несовершеннолетних должна строиться не только на уголовном преследовании, но и на сочетании превентивных мер, платформенного регулирования, безопасного проектирования цифровых сервисов, образовательных программ и международного сотрудничества. Именно такой комплексный подход, при котором уголовное право выступает как крайнее средство, должен определять дальнейшее развитие законодательства Республики Казахстан.

Доктринальные исследования информационной безопасности несовершеннолетних в цифровой среде формируют теоретическую основу для развития правового регулирования. В российской и казахстанской юридической науке обоснована необходимость выделения информационно-психологической безопасности несовершеннолетних как самостоятельной правовой категории, обусловленной особыми различиями в воздействии цифровой среды на формирующуюся личность ребенка по сравнению со взрослым человеком [12, с. 45]. Исследователи подчеркивают необходимость постоянного обновления правового регулирования с учетом быстрого развития технологий и появления новых угроз: если законодательство фиксирует перечень конкретных деяний, оно неизбежно отстает от технологической реальности; если же оно оперирует чрезмерно абстрактными категориями, возникают проблемы правовой определенности. Согласно исследованию И.Л. Бачило, развитие информационных технологий неизбежно связано с необходимостью балансирования между свободой информации и защитой уязвимых категорий населения, прежде всего несовершеннолетних [13, с. 112]. Указанная дилемма приобретает особую остроту в условиях глобального характера информационного пространства, когда правовое регулирование одного государства может быть легко нейтрализовано посредством использования серверов и сервисов, действующих в других юрисдикциях.

Изучение международного опыта имеет непосредственное значение с точки зрения законодательства Республики Казахстан. Закон Республики Казахстан «О защите детей от информации, причиняющей вред их здоровью и развитию» от 2 июля 2018 г. определяет информационную безопасность детей как обеспечение защиты прав и законных интересов детей от информации, причиняющей вред их здоровью и развитию [14].

Статьи 39 и 39-1 Закона Республики Казахстан «О правах ребенка в Республике Казахстан» от 8 августа 2002 г. устанавливают режим защиты ребенка в информационном пространстве и государственный контроль за его соблюдением. Введение в 2024 г. статьи 127-2 Кодекса Республики Казахстан об административных правонарушениях, устанавливающей ответственность за

киберзапугивание в отношении несовершеннолетних, является закономерным и конституционно значимым шагом. Обоснованно заключить, что действующее законодательство Казахстана требует системного развития с учетом общепринятых направлений, выявленных на основе анализа международного опыта и существующих пробелов. В их числе – введение уголовной ответственности за онлайн-груминг в качестве самостоятельного состава преступления, установление обязанностей платформ по минимизации рисков для несовершеннолетних, внедрение требований к стандартам верификации возраста и развитие международного сотрудничества при расследовании трансграничных киберпреступлений.

Трансграничный характер киберпреступности осложняет защиту несовершеннолетних, поскольку правонарушитель, сервер и жертва могут находиться в разных государствах, а традиционные механизмы международной правовой помощи нередко оказываются слишком медленными для работы с цифровыми доказательствами. Хотя Второй дополнительный протокол к Будапештской конвенции 2022 г. направлен на упрощение трансграничного доступа к таким данным, его эффективность зависит от широкой ратификации и практического применения. Одновременно высокая латентность киберпреступлений против детей обусловлена страхом потерпевших, недостаточной осведомленностью взрослых, сложностями фиксации цифровых следов и нехваткой у компетентных органов необходимых технических ресурсов и специальных навыков.

Кроме того, квалификация киберпреступлений против несовершеннолетних создает трудности в силу новизны таких деяний и затрудняет формирование устоявшейся судебной практики. При этом эффективность уголовно-правовой охраны определяется не только качеством законодательных норм, но и уровнем подготовки кадров, техническим оснащением соответствующих органов и готовностью судов к рассмотрению дел с цифровыми доказательствами.

Особую сложность представляет проблема влияния генеративного искусственного интеллекта на информационную безопасность несовершеннолетних. Развитие технологий создания изображений позволяет формировать реалистичные изображения сексуального насилия над детьми без участия реальных детей, что ставит перед законодателем вопрос о криминализации подобных материалов. Ряд юрисдикций, включая Великобританию и отдельные штаты США, распространяют уголовную ответственность на синтетический контент, однако данный подход пока не является общепринятым.

Аргументы в пользу криминализации основаны на том, что такие материалы нормализуют сексуальную эксплуатацию детей и могут использоваться в процессе груминга; контраргументы указывают на проблемы установления пределов уголовно-правового запрета и соблюдения гарантий свободы выражения. Из этого следует, что технологическое развитие опережает правовое регулирование, а законодателям предстоит адаптировать уголовно-правовые категории к реальности, в которой границы между реальным и синтетическим контентом становятся все менее различимыми.

В современной доктрине и законодательной практике все большее значение придается ответственности цифровых платформ за обеспечение информационной безопасности несовершеннолетних. Традиционная модель, основанная преимущественно на уголовном преследовании отдельных правонарушителей, уже недостаточна, поскольку значительная часть рисков формируется и распространяется через платформы, контролирующие цифровую среду общения и потребления контента. Поэтому современный регуляторный подход исходит из того, что технологические посредники должны нести самостоятельные обязанности по защите детей, включая реализацию принципа «безопасности по умолчанию», при котором цифровые сервисы изначально проектируются с максимальным уровнем защиты несовершеннолетних.

Вместе с тем возложение регуляторных функций на цифровые платформы ставит ряд проблем, требующих критического осмысления. Прежде всего возникает вопрос о соразмерности требований и их влиянии на права несовершеннолетних. Как подчеркивает С. Ливингстон, общество не может ставить цели защиты детей ценой ограничения их прав и свобод, а также посредством политики, которая, пусть и непреднамеренно, стимулирует бизнес к исключению детей из цифровых услуг [4, с. 12]. Чрезмерно строгие требования к верификации возраста и модерации контента могут привести к тому, что платформы будут полностью ограничивать доступ несовершеннолетних, лишая их возможностей, предоставляемых цифровой средой. Кроме

того, делегирование функций контроля частным компаниям ставит вопросы прозрачности принимаемых решений, права на обжалование и демократической подотчетности. Предполагается, что оптимальная модель должна устанавливать четкие стандарты безопасности, предоставляя платформам определенную свободу в выборе технических средств их реализации при ответственном независимом аудите и контроле со стороны регулирующего органа.

Процессы датафикации детства, то есть массового сбора и анализа данных о детях, бросают вызов традиционным представлениям об информационной безопасности несовершеннолетних. Персональные данные детей перемещаются не только через социальные сети и развлекательные платформы, но и через образовательные сервисы, мобильные приложения и устройства умного дома. Совокупность этих данных создает детальный цифровой профиль человека, который может быть использован в коммерческих, манипулятивных или противоправных целях. Действующее законодательство большинства государств не в полной мере учитывает риски, связанные с агрегацией данных из различных источников и их долгосрочным хранением.

С нашей точки зрения, правовое регулирование защиты данных о несовершеннолетних должно учитывать не только актуальные риски, но и потенциальные последствия формирования устойчивого массива цифровых данных, который может повлиять на жизнь человека далеко за пределами периода несовершеннолетия: при приеме на работу, получении образования, страховании, доступе к социальным услугам и в иных ситуациях, где алгоритмический анализ способен привести к неблагоприятным решениям на основании информации, собранной в детстве без осознанного согласия.

Заключение

Таким образом, для Республики Казахстан, правовая система которой сочетает элементы континентальной традиции с собственной национальной спецификой, наиболее продуктивным представляется избирательное заимствование эффективных инструментов из различных юрисдикций с учетом национальных условий и международных обязательств государства. Особый интерес в этом контексте представляет соотношение уголовно-правовых и регуляторных принципов, уровень ответственности отдельных секторов за обеспечение безопасности детей и роль международного сотрудничества в противодействии трансграничным угрозам.

Предлагаем следующие меры: закрепить в уголовном законодательстве самостоятельный состав онлайн-груминга. Необходимо криминализировать установление взрослым лицом через Интернет, мессенджеры, игровые чаты и иные цифровые сервисы доверительного контакта с несовершеннолетним в целях сексуальной эксплуатации, вовлечения в изготовление интимных материалов, склонения к встрече либо иным формам противоправного воздействия. Это позволит пресекать опасное поведение на ранней стадии, не дожидаясь более тяжких последствий.

ЛИТЕРАТУРА

- 1 Международный союз электросвязи. Измерение цифрового развития: факты и цифры 2023 года. – Женева: Международный союз электросвязи, 2023. URL: <https://www.itu.int/itu-d/reports/statistics/facts-figures-2023/> (дата обращения: 10.01.2026).
- 2 Конвенция о правах ребенка: принята резолюцией Генеральной Ассамблеи ООН 44/25 от 20 ноября 1989 г. // United Nations Treaty Collection. – United Nations, Treaty Series. 2023. Vol. 1577. P. 3. URL: https://treaties.un.org/pages/ViewDetails.aspx?chapter=4&mtdsg_no=IV-11&src=IND (дата обращения: 10.01.2026).
- 3 Комитет ООН по правам ребенка. Замечание общего порядка № 25 (2021) о правах детей в связи с цифровой средой: CRC/C/GC/25: 2 марта 2021 г. – 24 с. URL: <https://digitallibrary.un.org/record/3906061> (дата обращения: 10.01.2026).
- 4 Livingstone S. Realizing Children's Rights in Relation to the Digital Environment, European Review. 2021, vol. 29, no. 1, pp. 20–33. URL: <https://doi.org/10.1017/S106279872000054X> (accessed: 08.06.2026).
- 5 Конвенция о киберпреступности: принята Советом Европы 23 ноября 2001 г.: ETS № 185. – Будапешт, 2001. URL: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185> (дата обращения: 10.01.2026).

- 6 Brenner S. W. *Cybercrime: Criminal Threats from Cyberspace*. Santa Barbara: Praeger, 2010. 296 p. URL: <https://www.bloomsbury.com/us/cybercrime-9780313365478/> (accessed: 10.01.2026).
- 7 Конвенция Совета Европы о защите детей от сексуальной эксплуатации и сексуального насилия: принята 25 октября 2007 г.: CETS № 201. – Лансароте, 2007. URL: <https://www.coe.int/en/web/children/lanzarote-convention> (дата обращения: 10.01.2026).
- 8 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) // Official Journal of the European Union. 2022. L 277. 27 October. P. 1–102. URL: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng> (accessed: 11.01.2026).
- 9 United States Code. Title 18. Part I. Chapter 110. Sexual Exploitation and Other Abuse of Children: 18 U.S.C. §§ 2251–2252A. URL: <https://www.law.cornell.edu/uscode/text/18/part-I/chapter-110> (accessed: 11.01.2026).
- 10 Online Safety Act 2023: 2023 Chapter 50. London: The Stationery Office, 2023. URL: <https://www.legislation.gov.uk/ukpga/2023/50> (accessed: 11.01.2026).
- 11 Strafgesetzbuch (StGB): in der Fassung der Bekanntmachung vom 13 November 1998 (BGBl. I S. 3322), zuletzt geändert durch Gesetz. URL: <https://www.gesetze-im-internet.de/stgb/> (accessed: 11.01.2026).
- 12 Рыдченко К.Д. Государственная система защиты несовершеннолетних от воздействия вредоносной информации: монография. – М.: ЮНИТИ-ДАНА, 2018. URL: <https://cyberleninka.ru/article/n/2018-03-018-rydchenko-k-d-gosudarstvennaya-sistema-zaschity-nesovershennoletnih-ot-vozdeystviya-vredonosnoy-informatsii-monografiya-m> (дата обращения: 14.01.2026).
- 13 Бачило И.Л. Информационное право : учебник для вузов. – 5-е изд., перераб. и доп. – М.: Издательство Юрайт, 2021. – 419 с. URL: <https://urait.ru/bcode/468354> (дата обращения: 14.01.2026).
- 14 О защите детей от информации, причиняющей вред их здоровью и развитию: Закон Республики Казахстан от 2 июля 2018 года № 169-VI ЗРК // ИПС «Әділет». URL: <https://adilet.zan.kz/rus/docs/Z1800000169> (дата обращения: 10.01.2026).
- 15 Об административных правонарушениях: Кодекс Республики Казахстан от 5 июля 2014 года № 235-V ЗРК // ИПС «Әділет». URL: <https://adilet.zan.kz/rus/docs/K1400000235> (дата обращения: 10.01.2026).

REFERENCES

- 1 Mezhdunarodnyj sojuz jelektrosvjazi. Izmerenie cifrovogo razvitija: fakty i cifry 2023 goda. – Zheneva : Mezhdunarodnyj sojuz jelektrosvjazi, 2023. URL: <https://www.itu.int/itu-d/reports/statistics/facts-figures-2023/> (data obrashhenija: 10.01.2026) (In Russian)
- 2 Konvencija o pravah rebenka: prinjata rezoljuciej General'noj Assamblei OON 44/25 ot 20 nojabrja 1989 g. // United Nations Treaty Collection. United Nations, Treaty Series. 2023. Vol. 1577. P. 3. URL: https://treaties.un.org/pages/ViewDetails.aspx?chapter=4&mtdsg_no=IV-11&src=IND (data obrashhenija: 10.01.2026) (In Russian)
- 3 Komitet OON po pravam rebenka. Zamechanie obshhego porjadka No. 25 (2021) o pravah detej v svjazi s cifrovij sredoj: CRC/C/GC/25: 2 marta 2021 g. 24 p. URL: <https://digitallibrary.un.org/record/3906061> (data obrashhenija: 10.01.2026) (In Russian)
- 4 Livingstone S. (2021) Realizing Children's Rights in Relation to the Digital Environment, *European Review*, vol. 29, no. 1, pp. 20–33. DOI: 10.1017/S106279872000054X. URL: <https://doi.org/10.1017/S106279872000054X> (accessed: 08.06.2026) (In English)
- 5 Konvencija o kiberprestupnosti : prinjata Sovetom Evropy 23 nojabrja 2001 g.: ETS No. 185. Budapesht, 2001. URL: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treaty-num=185> (data obrashhenija: 10.01.2026) (In Russian)
- 6 Brenner S.W. (2010) *Cybercrime: Criminal Threats from Cyberspace*. Santa Barbara : Praeger. 296 p. URL: <https://www.bloomsbury.com/us/cybercrime-9780313365478/> (accessed: 10.01.2026) (In English)
- 7 Konvencija Soveta Evropy o zashhite detej ot seksual'noj jekspluatacii i seksual'nogo nasilija: prinjata 25 oktjabrja 2007 g.: CETS No. 201. Lansarote, 2007. URL: <https://www.coe.int/en/web/children/lanzarote-convention> (data obrashhenija: 10.01.2026) (In Russian)
- 8 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) // Official Journal of the European Union. 2022. L 277. 27 October. P. 1–102. URL: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng> (accessed: 11.01.2026) (In English)
- 9 United States Code. Title 18. Part I. Chapter 110. Sexual Exploitation and Other Abuse of Children: 18 U.S.C. §§ 2251–2252A. URL: <https://www.law.cornell.edu/uscode/text/18/part-I/chapter-110> (accessed: 11.01.2026) (In English)

10 Online Safety Act 2023: 2023 Chapter 50. London: The Stationery Office, 2023. URL: <https://www.legislation.gov.uk/ukpga/2023/50> (accessed: 11.01.2026) (In English)

11 Strafgesetzbuch (StGB): in der Fassung der Bekanntmachung vom 13 November 1998 (BGBl. I S. 3322), zuletzt geändert durch Gesetz. URL: <https://www.gesetze-im-internet.de/stgb/> (accessed: 11.01.2026) (In German)

12 Rydchenko K.D. (2018) Gosudarstvennaya sistema zashhity nesovershennoletnih ot vozdejstviya vredonosnoj informacii: monografiya. M.: JuNITI-DANA. URL: <https://cyberleninka.ru/article/n/2018-03-018-rydchenko-k-d-gosudarstvennaya-sistema-zaschity-nesovershennoletnih-ot-vozdeystviya-vredonosnoy-informatsii-monografiya-m> (data obrashheniya: 14.01.2026) (In Russian)

13 Bachilo I.L. (2021) Informacionnoe pravo : uchebnik dlja vuzov. 5-e izd., pererab. i dop. M. : Izdatel'stvo Jurajt. 419 p. URL: <https://urait.ru/bcode/468354> (data obrashheniya: 14.01.2026) (In Russian)

14 O zashhite detej ot informacii, prichinjajushhej vred ih zdorov'ju i razvitiju : Zakon Respubliki Kazahstan ot 2 ijulja 2018 goda No. 169-VI ZRK // IPS «Әdilet». URL: <https://adilet.zan.kz/rus/docs/Z1800000169> (data obrashheniya: 10.01.2026) (In Russian)

15 Ob administrativnyh pravonarushenijah : Kodeks Respubliki Kazahstan ot 5 ijulja 2014 goda No. 235-V ZRK // IPS «Әdilet». URL: <https://adilet.zan.kz/rus/docs/K1400000235> (data obrashheniya: 10.01.2026) (In Russian)

ХАСАНОВА В.В.,^{*1}

З.Ф.М.

*e-mail: vikakiper85@bk.ru

ORCID ID 0000-0001-5579-1565

БЕГИМБАЕВ С.А.,²

З.Ф.К., аға оқытушы.

e-mail: begimbaev.serik@mail.ru

ORCID ID: 0009-0008-1383-9223

¹ҚР ПМ М. Бөкенбаев атындағы

Ақтөбе заң институты,

Ақтөбе қ., Қазақстан

²Алматы гуманитарлық-экономикалық

университеті,

Алматы қ., Қазақстан

КӘМЕЛЕТКЕ ТОЛМАҒАНДАРДЫҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІ: ХАЛЫҚАРАЛЫҚ АКТІЛЕР ЖӘНЕ ШЕТ ЕЛДЕРДІҢ ҚЫЛМЫСТЫҚ ЗАҢНАМАСЫН САЛЫСТЫРМАЛЫ-ҚҰҚЫҚТЫҚ ТАЛДАУ

Андатпа

Мақалада цифрлық ортадағы ақпараттық қатерлерден кәмелетке толмағандарды халықаралық-құқықтық және ұлттық қорғаудың көпдеңгейлі жүйесінің қалыптасуы зерттеледі. Өзектілігі цифрлық коммуникациялардың балалар мен жасөспірімдердің әлеуметтенуінің дербес кеңістігіне айналуына, ал қатерлердің көбіне жасырын коммуникациялық нысанда іске асуына байланысты айқындалады (кибербуллинг, онлайн-груминг, деструктивті және сексуалдандырылған контентті тарату, дербес деректерді заңсыз пайдалану), бұл оларды ерте анықтауды және құқықтық бағалауды қиындатады. Зерттеудің мақсаты негізгі халықаралық стандарттарды айқындау және әртүрлі юрисдикцияларда қалыптасып жатқан реттеушілік және қылмыстық-құқықтық ден қою модельдерін салыстыру болып табылады. Әдіснамалық негіз халықаралық және ұлттық актілерді формальды-заңдық және герменевтикалық талдауды, мемлекет пен цифрлық делдалдар міндеттерінің бөлінуін бағалаудағы жүйелі және құрылымдық-функционалдық тәсілдерді, сондай-ақ ортақ үрдістер мен айырмашылықтарды айқындауға арналған салыстырмалы-құқықтық әдісті қамтиды (оның ішінде Еуропа Кеңесінің киберқылмысқа қарсы іс-қимыл және балаларды сексуалдық қанаудан қорғау жөніндегі стандарттары). Қорғаудың қазіргі заманғы моделі барған сайын тек қылмыстық құдалаудан платформаларды криминализациялау мен превентивтік реттеуді ұштастыруға қарай ығысып бара жатқаны көрсетілген.

Тірек сөздер: кәмелетке толмағандардың ақпараттық қауіпсіздігі, цифрлық орта, киберқатерлер, онлайн-груминг, кибербуллинг, балалардың дербес деректері, халықаралық стандарттар.

KHASSANOVA V.V.,*¹

master of law.

*e-mail: vikakiper85@bk.ru

ORCID ID: 0000-0001-5579-1565

BEGIMBAYEV S.A.,²

c.l.s., senior lecturer.

e-mail: begimbaev.serik@mail.ru

ORCID ID: 0009-0008-1383-9223

¹Aktobe Law Institute
of the Ministry of Internal Affairs of the

Republic of Kazakhstan
named after M. Bukenbaev,
Aktobe, Kazakhstan

²Almaty Humanities and
Economics University,
Almaty, Kazakhstan

INFORMATION SECURITY OF MINORS: INTERNATIONAL ACTS AND COMPARATIVE LEGAL ANALYSIS OF CRIMINAL LEGISLATION OF FOREIGN COUNTRIES

Abstract

The article examines the formation of a multi-level system of international legal and national protection of minors from information threats in the digital environment. The relevance of the study is by the fact that digital communications have become an independent space of socialization for children and adolescents, while risks are often realized in a hidden communicative form (cyberbullying, online grooming, dissemination of destructive and sexualized content, unlawful use of personal data), which complicates early detection and legal assessment. The purpose of the study is to identify key international standards and to compare the regulatory and criminal law models of response being formed in different jurisdictions. The methodological framework includes formal legal and hermeneutic analysis of international and national acts, systemic and structural-functional approaches to assessing the distribution of duties between the state and digital intermediaries, as well as the comparative legal method for identifying common trends and differences (including the standards of the Council of Europe on cybercrime and the protection of children against sexual exploitation). It is shown that the modern model of protection is increasingly shifting from exclusively criminal prosecution to a combination of criminalization and preventive regulation of platforms.

Keywords: minors' information security, digital environment, cyber threats, online grooming, cyberbullying, children's personal data, international standards.

Дата поступления статьи в редакцию: 01.04.2026