

ОРГАНИЗАЦИЯ ПРОКУРОРСКОГО НАДЗОРА ЗА ИСПОЛНЕНИЕМ ЗАКОНОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НЕСОВЕРШЕННОЛЕТНИХ

Ч.И. Арабаев¹, д-р юрид. наук, академик, профессор, вице-президент НАН КР, директор

И.С. Маатов², соискатель учёной степени канд. юрид. наук

Улукбек Суеркулов³, соискатель учёной степени канд. юрид. наук

¹Институт государства и права Национальной академии наук Кыргызской Республики

²Национальная академия наук Кыргызской Республики

³Ошский государственный университет

^{1,2}(Кыргызстан, г. Бишкек)

³(Кыргызстан, г. Ош)

DOI:10.24412/2500-1000-2025-2-3-175-180

Аннотация. Современная цифровая среда создает новые вызовы для защиты информационной безопасности несовершеннолетних, включая распространение деструктивных интернет-игр, кибербуллинг и вовлечение детей в экстремистскую деятельность. Прокурорский надзор за исполнением законодательства в данной сфере становится ключевым инструментом предупреждения и пресечения угроз. В статье анализируются правовые механизмы защиты детей в Кыргызстане и международный опыт регулирования контента, влияющего на психику подростков. Отмечается необходимость усиления контроля за цифровой средой, а также профилактической работы с молодежью и родителями.

Ключевые слова: информационная безопасность, прокурорский надзор, несовершеннолетние, интернет-угрозы, деструктивный контент, цифровая среда.

Информационная безопасность представляет собой состояние защищенности информационной среды общества, при котором обеспечивается ее устойчивость к внешним и внутренним угрозам, предотвращаются негативные воздействия на критические информационные системы, а также гарантируется доступность, целостность и конфиденциальность данных. В условиях стремительной цифровизации информация перестала быть исключительно инструментом управления, а превратилась в самостоятельную социально-экономическую категорию, обладающую стратегическим значением [12].

В Кыргызской Республике информационная безопасность является неотъемлемой частью национальной безопасности, а ее правовое регулирование основывается на Конституции Кыргызской Республики, Концепции национальной безопасности, а также ряде специализированных законов, включая законы «О защите государственных секретов Кыргызской Республики», «О средствах массовой информации», «Об электронном управлении» и других [3, с. 165]. Важным нормативным документом, определяющим стратегические подходы к обеспечению информа-

ционной безопасности, является Концепция информационной безопасности Кыргызской Республики на 2019-2023 годы, утвержденная постановлением Правительства Кыргызской Республики от 3 мая 2019 года № 209. Концепция устанавливает основные направления защиты информационной сферы, предусматривая меры по прогнозированию, выявлению, предупреждению и нейтрализации информационных угроз, а также цифровую трансформацию государственных и муниципальных услуг, включая проекты «Цифровой парламент», «Безопасный город» и «Единый реестр преступлений» [2].

Развитие информационно-коммуникационных технологий и их интеграция во все сферы деятельности общества требуют усиленной защиты национальных интересов в информационной среде. В соответствии с Концепцией информационной безопасности, к ключевым методам обеспечения информационной безопасности относятся правовые, организационно-технические и экономические меры, направленные на защиту информационной инфраструктуры, а также формирование безопасного цифрового пространства. Важную роль в регулировании этой сферы играет За-

кон Кыргызской Республики «Об электронном управлении», который устанавливает порядок взаимодействия государственных органов, организаций и граждан в рамках цифрового документооборота, обеспечивая правовую защиту электронных данных и предотвращая их неправомерное использование [1].

В последнее десятилетие деструктивные интернет-явления приобрели массовый характер, став серьезной угрозой для несовершеннолетних. Среди наиболее известных таких явлений – «Синий кит», «Момо», «Красная сова» и другие. Их суть заключается в манипуляции сознанием подростков с целью доведения их до членовредительства или самоубийства. Организаторы подобных сообществ действуют анонимно, используя социальные сети и мессенджеры для контакта с жертвами.

Они постепенно вводят подростков в психологическую зависимость, задавая им различные задания, начиная с безобидных, но постепенно переходя к опасным. Финальным этапом становится принуждение к суициду. Деятельность таких сообществ приобрела широкую огласку после серии трагических случаев, особенно среди подростков России и стран СНГ [6, с. 195].

«Синий кит» – так называемая «игра», распространяемая через социальные сети и мессенджеры, в которой подростков подталкивали к выполнению опасных заданий, кульминацией которых становилось самоубийство. В Кыргызстане в 2017 году Генеральная прокуратура зафиксировала 22 случая вовлечения несовершеннолетних в подобные «игры». Аналогичные случаи происходили и в других странах, например, в США, где дело «Слендермена» продемонстрировало опасность влияния интернет-мемов на психику детей. Подобные явления указывают на необходимость ужесточения контроля за контентом, который может провоцировать подростков на саморазрушительные действия [4, с. 173].

В целях борьбы с интернет-угрозами в Кыргызстане и других странах приняты меры законодательного регулирования. Так, в Кыргызской Республике Генеральная прокуратура совместно с межведомственной рабочей группой инициировала блокировку сайтов, распространяющих подобный контент, ссылаясь на Закон КР «О защите детей от информации, причиняющей вред их здоровью и разви-

тию». В России в 2017 году в Уголовный кодекс была внесена статья 110.1 («Склонение к совершению самоубийства»), предусматривающая уголовную ответственность за доведение до суицида с использованием интернета. В Казахстане аналогичные действия регулируются статьей 105 УК РК, в рамках которой за доведение до самоубийства, в том числе через телекоммуникационные сети, предусмотрены суровые наказания [7, с. 45].

В 2017 году китайские власти приняли жесткие меры по борьбе с этой игрой: блокировались ключевые слова, связанные с «Синим китом», удалялись группы в социальных сетях, а подростки, причастные к распространению экстремистских идей, подвергались аресту. Министерство общественной безопасности КНР совместно с другими правоохранительными органами ввело мониторинг социальных сетей и мессенджеров для предотвращения распространения подобных игр. Согласно статье 287 Уголовного кодекса КНР, за распространение вредоносного контента в интернете предусмотрено уголовное наказание, а в особо тяжких случаях – длительное лишение свободы. Несмотря на принятые меры, общественность обеспокоена тем, что запреты могут лишь усилить интерес к игре среди подростков, что требует дополнительной работы с молодежью и их родителями в профилактических целях [13].

В Кыргызстане в 2018 году появилось еще одно опасное явление – игра «Момо», распространяемая через мессенджер WhatsApp. МВД Кыргызской Республики зафиксировало случаи получения подростками пугающих сообщений с угрозами и принуждением к выполнению заданий, ведущих к членовредительству и суициду. В связи с этим, органы правопорядка рекомендовали родителям внимательно следить за контактами детей в социальных сетях и мессенджерах. Межведомственная группа при Генеральной прокуратуре Кыргызской Республики в 2019 году заблокировала несколько ресурсов, распространяющих информацию о «Момо», а также провела информационную кампанию среди населения [11]. Детские психологи указывают, что в группе риска находятся дети, испытывающие нехватку внимания со стороны родителей, что подчеркивает важность семейного общения и воспитания [10].

Онлайн-груминг, кибербуллинг и вовлечение детей в экстремистскую деятельность представляют серьезные угрозы для безопасности несовершеннолетних в цифровой среде. Онлайн-груминг подразумевает манипуляцию и установление доверительных отношений с детьми с целью их сексуальной эксплуатации. Согласно докладу Всемирной организации здравоохранения (ВОЗ) за 2022 год, жертвами онлайн-груминга ежегодно становятся тысячи детей, а кибербуллинг, который выражается в угрозах, преследовании и публичном унижении в сети, может привести к психологическим расстройствам и социальному отчуждению подростков. Согласно исследованию ЮНИСЕФ, каждый третий ребенок сталкивается с кибербуллингом, а каждый пятый из-за этого пропускает школу.

Вовлечение несовершеннолетних в экстремистскую деятельность через цифровые платформы также стало одной из актуальных проблем, требующих жестких мер со стороны государства и международного сообщества. Террористические и радикальные группы используют социальные сети, видеохостинги и мессенджеры для вербовки детей и подростков, манипулируя их сознанием и вовлекая в преступную деятельность. Согласно отчету Управления ООН по наркотикам и преступности (УНП ООН), число несовершеннолетних, завербованных онлайн, за последние годы значительно возросло, что требует усиления мер по цифровой безопасности [8, с. 149].

Защита детей от вредоносного контента на международном уровне регламентируется рядом ключевых нормативно-правовых актов, основным из которых является Конвенция ООН о правах ребенка (1989). Согласно ее положениям, государствам-участникам пред-

писывается создавать механизмы защиты несовершеннолетних от информации, способной причинить вред их физическому, психическому или нравственному развитию. В статье 17 Конвенции подчеркивается важность обеспечения доступа детей к информации, соответствующей их возрастным потребностям, при одновременном введении мер, препятствующих распространению вредоносного контента [6, с. 195].

Важную роль в обеспечении информационной безопасности несовершеннолетних играют и другие международные акты, такие как Международный пакт о гражданских и политических правах (1966), Европейская конвенция о защите прав человека и основных свобод (1950) и Рекомендации Комитета министров Совета Европы № R (97)19 «О демонстрации насилия в электронных средствах массовой информации» (1997).

Помимо универсальных международных стандартов, разработанных в рамках ООН и Совета Европы, существуют специализированные механизмы защиты, регулирующие деятельность медиа, цифровых платформ и рекламных структур. Так, «Пекинские правила» (1985) и «Эр-Риядские принципы» (1990) акцентируют внимание на необходимости минимизации негативного воздействия информации, особенно в отношении несовершеннолетних, находящихся в социально уязвимом положении. Международный кодекс рекламной практики Международной торговой палаты устанавливает ограничения на рекламу, способную навредить детям, а Европейская конвенция о трансграничном телевидении (1989) вводит принципы регулирования трансляции контента с элементами насилия или порнографии [10].

Таблица 1. Меры по обеспечению информационной безопасности

Страна	Основные законы и меры	Органы контроля	Технические средства	Примечания
Кыргызстан	- Концепция информационной безопасности (2019-2023); - Закон «О средствах массовой информации»; - Закон «Об электронном управлении»; - Закон «О защите детей от информации, причиняющей вред их здоровью и развитию»	- Генеральная прокуратура КР - МВД КР - Государственный комитет национальной безопасности (ГКНБ) - Межведомственная рабочая группа	- Блокировка деструктивного контента; - Цифровой контроль над электронными данными; - Фильтрация контента в образовательных учреждениях	Внедрены проекты «Цифровой парламент», «Безопасный город», «Единый реестр преступлений»
Казахстан	- Закон «Об информатизации»; - Закон «О защите детей от информации, причиняющей вред их здоровью и развитию»; - Статья 105 УК РК (доведение до самоубийства); - Национальная концепция кибербезопасности «Киберщит Казахстана»	- КНБ РК (Комитет национальной безопасности) - МВД РК - Министерство цифрового развития, инноваций и аэрокосмической промышленности РК - Прокуратура РК	- Мониторинг и блокировка вредоносного контента; - Система интернет-фильтрации; - Центры оперативного реагирования на киберугрозы	Реализуется программа «Киберщит Казахстана» для защиты от кибератак и интернет-угроз
США	- Communication Decency Act (1996, признан неконституционным); - Children's Online Privacy Protection Act (1998, заблокирован судом); - Children's Internet Protection Act (CIPA, 2000)	- Таможенная служба США (Центр противодействия киберконтрабанде); - Подразделение защиты детей; - Федеральная комиссия по связи (FCC)	- Фильтрация контента в школах и библиотеках; - Система возрастных ограничений на ТВ	Введены штрафы за нарушение норм (пример – штраф Viacom за трансляцию откровенного контента)
Китай	- Закон о защите несовершеннолетних (1992); - Проект «Золотой щит» (с 2003 года); - Центр жалоб (с 2004 года)	- Министерство общественной безопасности - Государственное управление по делам интернет-информации; - Центр жалоб	- Великий китайский файрвол; - Фильтрация контента провайдерами	Самая жесткая система интернет-контроля, учитывает политический аспект
Россия	- Закон № 139-ФЗ (2012); - Закон № 436-ФЗ (2010); - Поправки в Кодекс об административных правонарушениях (2012); - Закон «Об информации» (2006)	- Роскомнадзор; - МВД РФ; - ФСБ РФ	- Единый реестр запрещенных сайтов; - Система возрастной маркировки контента (6+, 12+, 16+, 18+)	Реестр запрещенных сайтов работает на уровне провайдеров

В Кыргызской Республике цифровая трансформация общества открывает широкие возможности для обучения, саморазвития и коммуникации, но одновременно приводит к росту рисков, связанных с неконтролируемым распространением деструктивной информации, кибербуллинг, вовлечением несовершеннолетних в преступную деятельность и другими угрозами [2].

В условиях стремительной цифровизации и роста преступлений в интернете органы прокуратуры осуществляют надзор за соблюдением законодательства в сфере информационной безопасности, а также принимают меры прокурорского реагирования в случаях нару-

шения прав граждан и организаций. В соответствии со статьей 1 Конституционного Закона Кыргызской Республики «О прокуратуре Кыргызской Республики», прокуратура осуществляет надзор за точным исполнением законодательных актов, включая законы, регулирующие цифровое пространство.

Эффективное осуществление прокурорского надзора в цифровой среде требует адаптации к современным реалиям, что нашло отражение в недавних изменениях Уголовного кодекса КР и Уголовно-процессуального кодекса КР. В частности, введены новые составы преступлений, касающиеся незаконного доступа к компьютерной информации, распро-

странения вредоносных программ и цифрового мошенничества. Прокуратура, реализуя свои функции, взаимодействует с правоохранительными органами, уполномоченными в сфере кибербезопасности, такими как Государственный комитет национальной безопасности (ГКНБ) и Министерство внутренних дел (МВД), а также с международными организациями, специализирующимися на противодействии киберугрозам [13].

Прокурорский надзор за соблюдением законодательства в сфере защиты детей от информационных угроз играет ключевую роль в обеспечении прав несовершеннолетних на безопасное информационное пространство. В Кыргызской Республике основным нормативно-правовым актом, регулирующим данный вопрос, является Закон КР «О защите детей от информации, причиняющей вред их здоровью и развитию». В рамках прокурорского надзора осуществляется контроль за соблюдением норм этого закона государственными органами, учреждениями образования, СМИ и интернет-ресурсами. Особое внимание уделяется мониторингу информационной среды, включая контент, транслируемый на телевидении, в сети Интернет и в печатных изданиях. Органы прокуратуры обязаны выявлять и

пресекать распространение материалов, содержащих сцены насилия, пропаганду вредных привычек, суицидальных наклонностей, деструктивных культов и иных угроз для психического и морального развития детей [9, с. 68].

Резюмируя вышесказанное, информационная безопасность в Кыргызской Республике является важнейшим элементом национальной безопасности, требующим комплексного подхода к защите граждан и государства от цифровых угроз. Развитие технологий открывает новые возможности, но одновременно создает риски, связанные с распространением деструктивного контента, киберпреступностью и манипуляцией сознанием несовершеннолетних. Для эффективного противодействия этим вызовам государственные органы принимают правовые, технические и организационные меры, включая мониторинг интернет-пространства, блокировку опасных ресурсов и совершенствование законодательства. В условиях стремительной цифровизации особую роль играет прокурорский надзор, обеспечивающий контроль за исполнением нормативных актов в сфере кибербезопасности и защиту прав граждан в цифровой среде.

Библиографический список

1. Закон Кыргызской Республики от 19 июля 2017 года № 127 «Об электронном управлении» (в редакции Законов КР от 24 июля 2020 года № 94, 18 ноября 2022 года № 4).
2. Концепция информационной безопасности Кыргызской Республики на 2019-2023 годы: утверждена постановлением Правительства Кыргызской Республики от 3 мая 2019 года № 209. – Бишкек, 2019.
3. Буданов С.А., Гаврилов С.Т. Информационная безопасность несовершеннолетних: правовой аспект // Территория науки. – 2015. – № 2. – С. 165-169.
4. Куватпеков К.Б., Мамырганов М.Р. Эволюция уголовного законодательства Кыргызской Республики за «доведение до самоубийства»: сравнительно-правовой аспект // Вестник Академии государственного управления при Президенте Кыргызской Республики имени Жусупа Абдрахманова. – 2022. – № 29. – С. 173-177.
5. Рыбакова О.С. Безопасность несовершеннолетних в информационном обществе: анализ киберрисков и угроз // Мониторинг правоприменения. – 2020. – №2 (35). – С. 65-73.
6. Титор С.Е. Международные принципы защиты детей от деструктивной информации // Вестник Московского университета МВД России. – 2023. – № 3. – С. 195-199.
7. Турдубаева Р.Ш. Профилактика и коррекция агрессивного поведения подростков // Известия вузов Кыргызстана. – 2017. – № 5.
8. Цуканов А.Н., Вахрушев Г.Е. Международные стандарты защиты ребенка от негативной информации // Пробелы в российском законодательстве. Юридический журнал. – 2013. – № 3. – С. 149-155.
9. Шаршеналиев Ж.А. Место и роль прокуратуры в системе органов государственной власти Кыргызстана / Ж.А. Шаршеналиев, Г.С. Рыспаева // Вестник Кыргызского Национального Университета имени Жусупа Баласагына. – 2019. – № 4(100). – С. 116-120. – EDN EOLPJM.

10. Организация Объединённых Наций. Безопасность детей и молодежи в интернете. – [Электронный ресурс]. – Режим доступа: <https://www.un.org/ru/global-issues/child-and-youth-safety-online>.

11. Радио Азаттык. Опасная игра «Момо» и безопасность детей в интернете. – [Электронный ресурс]. – Режим доступа: https://rus.azattyk.org/a/kyrgyzstan_momo_bezопасnost/29441858.html.

12. Устинов Д. Сущность информационной безопасности / Д. Устинов // Международный журнал гуманитарных и естественных наук. – 2017. – № 12. – С. 146-151. – EDN YMGQWF.

13. Цифровой дозор. – [Электронный ресурс]. – Режим доступа: <https://slovo.kg/politika/cifrovoj-dozor/>.

ORGANISATION OF PROSECUTOR'S SUPERVISION OVER THE ENFORCEMENT OF LAWS IN THE SPHERE OF INFORMATION SECURITY OF MINORS

Ch.I. Arabaev¹, *Doctor of Law Sciences, Professor, Vice-President of the National Academy of Sciences of the Kyrgyz Republic, Director*

I.S. Maatov², *Applicant to the Candidate of Law Sciences*

U. Suerkulov³, *Applicant to the Candidate of Law Sciences*

¹**Institute of State and Law of the National Academy of Sciences of the Kyrgyz Republic**

²**National Academy of Sciences of the Kyrgyz Republic**

³**Osh State University**

^{1,2}**(Kyrgyzstan, Bishkek)**

³**(Kyrgyzstan, Osh)**

Abstract. *The modern digital environment creates new challenges for the protection of information security of minors, including the spread of destructive Internet games, cyberbullying and involvement of children in extremist activities. Prosecutor's supervision over the implementation of legislation in this area is becoming a key tool for preventing and combating threats. The article analyses the legal mechanisms of child protection in Kyrgyzstan and the international experience of regulating content that affects the psyche of adolescents. The necessity of strengthening control over the digital environment, as well as preventive work with young people and parents is noted.*

Keywords: *information security, prosecutor's supervision, minors, Internet threats, destructive content, digital environment.*