Митин А.Н.,
Урал мамлекеттик юридикалык университети,
башкаруунун теориясы жана
практикасы кафедрасынын башчысы,
экономика илимдеринин доктору, профессор
Митин А.Н.,
заведующий кафедрой
теории и практики управления,
профессор, доктор экономических наук
Уральский государственный юридический университет
ул. Комсомольская, 23, г. Екатеринбург, 620137
Mitin A.N.,
head of Department of theory and practice of management,
professor, doctor of economic sciences,
Ural State Law University
23 Komsomolskaya Str., Ekaterinburg, 620137;
e-mail: idom@usla.ru
tel.:+7-912-245-20-99
ORCID: 0000-003-1788-6736

УДК 343.2/.7

КИБЕР КУУГУНТУКТООГО КАРШЫ КҮРӨШҮҮ ЧӨЙРӨСҮНДӨГҮ МАМЛЕКЕТТИК САЯСАТ

ГОСУДАРСТВЕННАЯ ПОЛИТИКА В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСЛЕДОВАНИЯМ

STATE POLICIES IN THE FIELD OF COUNTERING CYBERBULLYING

Аннотация: статья посвящена исследованию государственной политики по решению проблем информационной безопасности и киберпреследования. Орудиями киберпреследования являются электронная почта, мессенджеры, форумы и чаты, социальные сети, смартфоны. Сеть позволяет злоумышленнику оставаться анонимным. Анализируется термин «киберпреследование» в исследованиях ученых и в законодательстве различных государств. Сформулированы предложения по внесению изменений в законодательство Российской Федерации и по созданию комплексной системы противодействия киберпреступлениям, в том числе киберпреследованиям, с участием международных организаций.

Annotation: The article is devoted to the study of state policies on the problems of infor-mation security and cyberbullying. The cyberbullying tools are e-mail, instant messengers, forums and chat rooms, social networks, smartphones. The network allows the attacker to remain anony-mous. The term “cyberbullying” is analyzed in the research of scientists and in the legislation of various states. The proposals for amendment to the legislation of the Russian Federation and for creation of a comprehensive

system of countering cybercrimes are formulated, including cyberbul-lying with the participation of international organizations.

Ключевые слова: информационная безопасность; киберпространство; киберпреступ-ления; киберпреследование; государственная политика; мировой опыт; результаты иссле-дования

Keywords: information security; cyberspace; cybercrime; cyberstalking; state policie;, global experience; research results.

Современный период развития человеческой цивилизации характеризуется стремительным ростом инновационных коммуникативных технологий. Информационный потенциала их настолько велик, что не только расширяет государственные возможности интеренет – управления, но и свидетельствуют о появлении принципиально иных, чем прежде, киберу-гроз для информационной безопасности как отдельного государства, так и и международного сообщества в целом.

Термины с приставкой «кибер» получили широкое употребление в международно-политическом дискурсе, они присутствуют в доктринальных документах не только государств, но и международных организаций, особенно военного назначения. «Кибервойна», «кибертерроризм», «кибератака», «киберпространство» стали реальностью, что свидетельствует о милитаризации Интернета и необходимости создания защитных механизмов от этих видов угроз. С одной стороны, это возможно осуществлять традиционно через государственные политики, но без ограничений за счет гражданских свобод, а с другой – через расширение управленческих воздействий с помощью как традиционных, так и новых форм государственного контроля. Не менее важна и третья сторона – правовая защита человека, организации и государства.

К традиционному контролю причисляются цензура, ограничения или прерывания Интернет-доступа, регулируемый импорт и экспорт соответствующих технологий для киберзащиты, фильтрация рекламной деятельности, противоправных призывов в Интернете и т. д.

Такие подходы могут привести к созданию правил международной координации через Интернет-сообщество. В свое время Россия и Китай даже выражали настроение о создании международного кодекса поведения в сфере информационной безопасности.

Индия, Бразилия и Южная Африка пошли по пути применения межправительственной модели с целью нормотворчества Интернет-сообщества с участием международных организаций и негосударственных заинтересованных структур. Есть страны, категорически отвергающие Интернет-цензуру. Таким образом, расширение и модификация традиционных форм контроля зависит от уровня развития в стране демократических институтов, исторического опыта, ментальности населения, соблюдения прав человека, социально-экономического развития, оснащенности информационно-коммуникационной сферы.

Здесь следует заметить, что в силу особенностей такого специфического ресурса, как информация, государство имеет крайне ограниченные возможности управления и контроля.

Расширение управленческих воздействий в целях укрепления информационной без-опасности может осуществляться и с менее жесткими ограничениями при использовании Интернет-ресурсов. И это тоже сильный аргумент, излагаемый в государственной политике. Это может осуществляться через расширение мониторинга Интернет-программ и некоторых сайтов с привлечением общественных институтов гражданского общества, последующими публичными дискуссиями на цифровых форумах. Основная идея таких организационных управляемых воздействий – значимость цифровой свободы и значимость ответственности в цифровом пространстве.

Цифровая свобода подразумевает традиционные права человека, право на свободу слова, которые в некоторых странах оцениваются выше, чем защита данных. Ответственность – правила, которыми должны оперировать, которых должны придерживаться все участники киберпространства. Хотя здесь с юридической стороны возникают проблемы конфиденциальности информации: в безграничном киберпространстве традиционные концепции юрисдикции основаны на суверенитете определенной территории.

Термин «киберпространство» описывает виртуальное пространство, в котором циркулируют электронные данные всех компьютеров мира [1], в нем же присутствуют и киберпреследования.

Правовая защита от киберпосягательств – не менее важный фактор государственной политики информационной безопасности. Например, в Индии, обсуждается государственной поли-

тики «Безопасность компьютерных сред и высокий уровень надежности электронных транзакций» [2]. В этом документе отмечается необходимость «защиты данных на этапе их обработки, хранения и передачи, а также защиты конфиденциальной личной информации с целью создания атмосферы доверия. Если для воздействия на человека или организацию требуются юридические усилия (как гражданского, так и уголовного характера), необходимо надлежащим образом собирать, сохранять и представлять электронные доказательства, соблюдая правила, действующие в соответствующей юрисдикции».

Опубликованная в 2010 г. Стратегия кибербезопасности Канады основывается на трех основных принципах:

защита правительственных систем;

сотрудничество с целью защиты ключевых информационных и телекоммуникационных систем, находящихся вне ведения федерального правительства;

обеспечение безопасности канадских граждан в онлайн-среде.

Третий принцип предусматривает вопросы защиты персональных данных.

Среди основных мероприятий государственной политики, которые сформулированы в Стратегии кибербезопасности Японии, предусмотрено решение задач информационной без-опасности общества и правовая защита личности. Подобные государственные политики изложены в конкретных документах Австралии, Израиля и других государств.

В Кыргызстане разработана Стратегия кибербезопасности страны на 2018-2023 годы. Это рамочный документ доктринального уровня, подготовленный с учетом международного опыта, который служит основой для формирования государственной политики в этой сфере [3].

Названные формы государственных политик сориентированы не только на создание си-стем информационной безопасности, но и на подавление различной криминальной активности в киберпространстве, для которой характерно совершение преступных деяний с помощью компьютера или смартфона. Такой вид преступлений называется киберпреступностью (англ. cybercrime).

Как отмечает Д. О. Крылов [4], сегодня не существует единого универсального определения этого термина, даже в разделе «Киберпреступность» на сайте Интерпола. В право-охранительной практике, как правило, различают два основных вида Интернет-преступлений.

«Advanced cybercrime» – высокотехнологичная преступность, представляющая собой изощренные атаки на аппаратные средства компьютера и программное обеспечение.

«Cyber-enabled crime» – преступность, использующая виртуальное пространство для совершения многих «традиционных» преступлений таких, как преступления против детей, финансовые преступления, кражи, мошенничество, киберпреследование, незаконные азартные игры, продажа поддельных лекарств и даже терроризм. В этом случае речь идет о новых возможностях совершения преступлений онлайн, которые становятся все более массовым и разрушительным [5].

Некоторые юристы считают, что их следует рассматривать как квалифицирующий при-знак обычных «традиционных» преступлений. При этом компьютер и его сети выступают в качестве предмета преступления или средства, на котором подготавливаются и осуществляются противоправные деяния.

В контексте нашего исследования особый интерес представляет один из таких видов Интернет-преступлений, который имеет название «cyberstalking» (киберпреследование). Это своего рода онлайн-домогательство, в котором жертва подвергается шквалу интернет-сообщений и сообщений электронной почты. Как правило, сталкеры знают своих жертв и вместо того, чтобы прибегать к личному выслеживанию, они используют для слежки Интернет.

В «классическом» варианте киберпреследования злонамеренную атаку ведет один человек с одного или нескольких источников, а сама схема напоминает ботсети [6]. По существу, это мотивированная атака, результатом которой является насилие против личности.

Исследователями из Государственного университета Сэми Хьюстона США проведено сравнение жертв обычного преследования и преследования через Интернет [7]. Оказалось людям, столкнувшимся с киберпреследованием и получавшим угрозы через Интернет, при-ходилось больше платить, чтобы справиться с проблемой. Кроме того, они дольше жили в страхе и чаще прибегали к самозащите по сравнению с теми, кто страдал от обычного преследования.

Без сомнения, киберпреследование нарушает границы человека и заставляет его использовать более разнообразные средства самозащиты. Реальное преследование кажется более опасным, но распространенность современных технологий привела к тому, что угрозы через Интернет беспокоят людей сильнее. Преследователям стало проще следить за жертвой, а жертвам, наоборот, сложнее себя защитить.

Анализ научных публикаций свидетельствует о различных формулировках, касающихся киберпреследования. Оно определяется как «вид системного преследования с использованием вычислительной техники, сочетающийся с явно выраженными или подразумеваемыми угрозами, вызывающими у жертвы чувство опасности [8, С. 44-48] и включает в себя ложные обвинения, клевету, навет, а также мониторинг, кражу личных данных, угрозы, вандализм, предложения секса, сбор информации, которая может быть использована для последующих угроз и преследования. Киберпреследование может проходить в реальном времени или в автономном режиме. Главная цель такого поведения – желание контролировать, запугать или воздействовать на жертву [9].

В научной статье Д. А. Андерсене [10] киберпреследование рассматривается как «разновидность» преступных деяний в сфере защиты персональных данных». Оно чаще всего проявляется как виртуальное, для которого, как и преследование в реальной жизни, характерно приставание (harassment) и одержимость преследователя своей жертвы. Преследование может фактически рассматриваться как форма этого незаконного приставания. Можно согласиться с этим утверждением, поскольку защита персональных данных является приоритетным направлением государственной политики, важной задачей операторов персональных данных в противодействие их незаконному распространению, копированию и сбору.

В исследовании киберпреследования П. Н. Кобец [11, С. 28] предлагает свое определение этого понятия: «Это использование информационно-коммуникационных технологий с целью вызвать раздражение, агрессию или беспокойство у людей. Такие домогательства могут включать следующие действия: отправку оскорбительного электронного сообщения, кражу идентификации, повреждение данных или оборудования. Такое киберпреследование обычно включает в себя сбор информации о жертве с помощью поисковиков, привлечение общественности и осквернение личности через форумы, блоги и социальные сети».

Рассматривая киберпреследование как информационное преступление,

А. А. Гребеньков [12, С. 201-202] считает, что оно может осуществляться с использованием средств анонимизации общения в течении длительного времени, в том числе не одним посягающим, а сразу несколькими, даже малознакомыми с жертвами и действующими из хулиганских или садистских побуждений. Свое суждение автор укрепляет ссылкой на другого исследователя, Е. И. Клочко [13, С. 69-72], который утверждает, что в процессе киберпреследования жертва оказывается лишенной как-то воздействовать на посягающих как правовыми, так и внеправовыми методами из-за сложностей с установлением их личности, отсутствием прямого правового запрета на подобное преследование. Последствия могут быть крайне тяж-кими, известны случаи совершения жертвами подобного преследования суицида.

А. А. Гребеньков [14, С. 69-72], основываясь на нормах УК РФ о преступлениях против личности, выделяет следующие наиболее опасные формы киберпреследования: а) доведение до самоубийства с использованием угроз и шантажа; б) истязание, то есть систематическое причинение психических страданий путем преследования; в) угроза убийством или причинением тяжкого вреда здоровью; г) клевета; д) понуждение к действиям сексуального характра.

В этой связи, для более эффективного противостояния этим преступлениям, им предлагается:

1. Включить в ст. 110 УК РФ указание на шантаж как на способ доведения до само-убийства.

2. Включить в ст. 117 УК РФ указание на анонимную или систематическую отправку электронных сообщений как способ причинения психических страданий.

3. Включить в ст. 119 УК РФ указание на то, что ответственность по ней наступает, если имелись основания опасаться осуществления этой угрозы, либо угрозы совершаются с использованием информационных технологий, информационно-телекоммуникационных си-стем и носят систематический характер.

4. Предусмотреть квалифицированный состав клеветы с использованием информационных технологий и информационно-телекоммуникационных систем, установить, что производство по данному составу осуществляется в частнопубличном порядке (чтобы обеспечить выявление виновного силами правоохранительных органов).

5. Включить в число иных действий сексуального характера, к которым может побуждаться потерпевший, в составе ст. 133 УК РФ, также создание материалов, содержащих изображение или описание действий сексуального характера (т. н. «секстинг»).

Дополнительного исследования заслуживает вопрос об установлении административной ответственности за иные формы киберпреследования.

Мировой опыт противодействия киберпреследований, в основном, фрагментарен, но свидетельствует, что кибербезопасность рассматривается все же как одна из государственных политик. Особым образом в них выделяется киберпреследования женщин и детей.

В январе 2006 г. Президентом США подписан закон «О защите женщин от насилия» [15]. В нем есть поправка, позволяющая наказать человека за анонимное преследование с использованием Интернета.

По-разному определяется объект киберпреступлений в уголовном законодательстве стран СНГ: Кыргызстан (глава 28, статьи 289-291); Россия (глава 28, статьи 272-274); Армения (раздел 9, глава 24, статьи 251-257) и др.

В них обнаруживается разнообразие подходов, а также закономерности по криминализации новых деяний. Но отдельных понятий по киберпреследованию в процессе исследования не обнаруживается. Вместе с тем, в США, почти у каждого штата есть закон, который к этому преступному деянию обращается [16].

Например, в штате Вашингтон (США) наказуемым признаётся отправка электронного сообщения жертве или третьему лицу с целью потревожить,запугать, причинить страдание или вызвать смущение, если: а) это сообщение содержит непристойные слова или изображения, либо предполагает совершение непристойного акта; б) совершается анонимно или систематически вне контекста диалога; в) сопряжено с угрозой причинения вреда потерпевшему, его близким или их имуществу. Максимальное наказание за данное деяние — до 1 года лишения свободы, а если оно совершается лицом, ранее судимым за преследование или сопряжено с угрозой убийством — до 5 лет лишения свободы [17].

По этому же пути развивается законодательство Индии. Многие положения системы информационной безопасности государств – членов ОДКБ комплексно отражают современные особенности по нейтрализации противоправных воздействий на киберпространство.

Изучение немногочисленных публикаций свидетельствует о том, что в настоящее время в тексте государственных политик ряда стран заложены принципы противодействия распространению противоправного контента, что повлияло на закрепление в национальных законодательствах норм, что киберпреследование является уголовно наказуемым деянием. Так, например, несмотря на то, что понятие «киберпреследование» законодательно в России не закреплено, в соответствии с действующим уголовным правом под преступлениями в сфере компьютерной информации понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом, которых является информация и компьютерные средства. Данная группа посягательств является институтом особенной части Уголовного кодекса РФ. Ответственность за совершение которых предусмотрено гл. 28. Они относятся к подинституту «Преступления против общественной безопасности и общественного порядка». Видовым объектом рассматриваемых преступлений являются общественные отношения, связанные с безопасностью информации и систем обработки информации с помощью ЭВМ. Согласно Уголовному кодексу РФ преступлениями в сфере компьютерной информации являются: неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных про-грамм (ст. 273 УК РФ), нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (с. 274 УК РФ).

Однако в законодательстве РФ отсутствует ответственность за преследование человека, а законодатель ограничился лишь несколькими нормами, запрещающими вмешательство в частную жизнь.

Результаты исследования свидетельствуют о том, что в условиях стремительного развития информационных технологий начинают меняться и приоритеты государственных политик относительно противодействия киберпреступлениям и такой новой формы преступно-го деяния, как киберпреследование. Его общественная опасность велика, а последствия неизбежно наносят существенный вред личным интересам и здоровью личности. Согласно Добровольной on-line системе сообщений существует база сведений и учета таких преступлений (Cybersnitch Voluntary Online Crime Reporting System). Преступления, связанные с Интернет, увеличиваются и включают такие потенциально опасные деяния, как электронное преследо-вание и террористические угрозы (полный список преступлений доступен на: www.cybersnitch.net/csinfo/csdatabase.asp).

Влияние новых принципов государственных политик в противодействии киберпреступ-ности позволяет изменять формы взаимоотношений IT-профессионалов, наиболее часто ответственных за обеспечение первой линии защиты от киберпреступлений и их выявления, а также работников правоохранительных органов: первые предлагают сегодня необходимый инструментарий, а вторые – расширяют формы сбора доказательств и методы предания суду правонарушителей в сфере информационной безопасности: каждый владеет своей «полови-ной ключа».

Законы об on-line преступлениях в настоящее время принимаются и обновляются во всех правовых системах. Они опираются на определения киберпреступности, предложенные на X Конгрессе ООН, на Конвенцию совета Европы по киберпреступности, рекомендации международных конференций по информационному управлению. Но в международном со-обществе остаются проблемы создания пригодной дефиниции киберпреступности и связан-ных с ней терминов, в том числе «киберпреступления».

Основной фактор здесь – юрисдикционная дилемма, при которой законы различных юрисдикций формируют термины по-разному, а сами киберпреступления совершаются в виртуальном пространстве.

В этом случае для государств требуется иметь если не одинаковые, то по крайней мере, существенно не отличающиеся определения «киберпреступления», которые могут быть предложены с участием международных организаций, включая ООН.

По мнению Д. Л. Шиндера в перечень насильственных или иных потенциально опасных преступлений следует включить: кибертерроризм; угрозу физической расправы; киберпреследование; детскую порнографию. Он считает, что киберпреследование должно быть признано как «форма электронного преследования, которая зачастую сопряжена с явно выраженными или подразумеваемыми физическими угрозами, создающими чувство опасности у жертвы» [18].

Государственная политика в борьбе с киберпреступностью должна быть социально значимой, стратегически сориентированной на защиту граждан. Общие принципы, обозначенные правовые средства – это только часть стратегии. А потому здесь требуется одновременно системный и комплексный подходы с участием международных организаций, комплекс правовых, технических, информационных и организационных мероприятий. Их поэле-ментная база может состоять из нескольких блоков:

- создание пригодной дефиниции киберпреступлений их категоризация, а также связанных с ними терминов, которые для различных юрисдикций не имели бы существенных отличий;

- определение факторов для определения приоритетов в преодолении киберпреступности (размер вреда, частота совершения, юрисдикция, сложность дела, социальные, экономические, политические аспекты и др.);

- создание системы статистических данных и определение субъектов борьбы с кибер-преступностью;

- формирование законов, их обеспечение, надзор за исполнением;

- формирование специальных программ обучения тех, кто участвует в предотвращении, обнаружении киберпеступлений, судебном преследовании тех, кто х совершил.

- обучение IT-профессионалов навыкам совместной деятельности с представителями правоохранительных органов в борьбе с киберпреступностью;

- создание специальных программ защиты граждан – пользователей сети Интернет от преступных киберпосягательств, в том числе киберпреследования, а также привлечение об-ществен-ных организаций, способствующих выявлению преступных деяний в киберпростран-стве, особенно из числа молодежных формирований.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ:

1. Гринберг, А. С. Информационный менеджмент [Электронный ресурс]: /А.С. Грин-берг. – Режим доступа: http:www.ngpedia.ru/pg6384876uMBWtVn0001082137. /3.06.2019/. - Загл. экрана.

2. Discussion draft on National Cyber Security Policy [Электронный ресурс]: // Govern-ment of India. Department of Electronics and Information Technology. – Режим доступа: http://diety.gov.in/hindi/sites/upload_files/dithindi/files/ncsp_060411.pgf /07.05.2019/. - Загл. с экрана.

3. Госкомсвязи внес на утверждение правительству стратегию кибербезопасности Кыргызстана [Электронный ресурс]: – Режим доступа: Knew.kg. /22.06.2018./ - Загл. с экрана.

4. Крылов, Д. О. К вопросу о терминологии в сфере киберпреступности (на материале английского языка) [Электронный ресурс]: Cybercrime [Электронный ресурс]. – Режим до-ступа: https://www.interpol.int/Crime-areas/Cybercrime/ Cybercrime /6.06.2019/

5. Cybercrime [Электронный ресурс]. – Режим доступа: https://www.interpol.int/Crime-areas/Cybercrime/ Cybercrime (дата обращения: 6.06.2019)

6. Что такое киберпреследование [Электронный ресурс]: - Режим доступа: https://unotices.com/page-answer.php?id=852. /24.09.2018/. - Загл. с экрана.

7. Киберпреследование опаснее реального [Электронный ресурс] - Режим доступа: https://health.mail.ru/news/kiberpresledovanie_opasnee_realnogo/. /26.10.2018/. - Загл. с экрана.

8. Осипенко, А. Л. Общественно опасная информация в сети Интернет: криминологическая оценка и проблемы организации противодействия [Текст]: /А.Л. Осипенко // Совре-менное право. 2007. - №12.

9. Никитина, Е. М. Международно-правовое сотрудничество государств в области борьбы с киберпреследованием женщин [Электронный ресурс]: /Е.М. Никитина. – Режим до-ступа: giefjournal.ru/node/877 . / 1.06.2019/. - Загл. с экрана.

10. Андерсене Д. А. Киберпреследование – разновидность преступных деяний в сфере защиты персональных данных [Электронный ресурс]. – Режим доступа: https://webmaster.yandex/siteinfo/?Sito=aphet.ua. - Загл. с экрана.

11. Кобец, П. Н. Противодействие угрозам кибersталкинга – важней проблеме, исследуемой в рамках совершенствования аспектов информационной безопасности регионов в условиях глобализации информационного пространства [Текст]: /П.Н. Кобец //Вестник При-камского социального института. 2017, - №1 (76).

12. Гребеньков, А. А. Киберпреследование как информационное преступление [Текст]: сб. статей /А.А. Гребеньков // Международная научно-практическая конференция «Новые информационные технологии в науке нового времени» 5 октября 2016 г., Волгоград. – Уфа: АЭТЕРНА, 2016.

13. Клочко, Е. И. Воздействие Интернета на суидальное поведение молодежи [Текст]: /Е.И. Клочко // Общество. Среда. Развитие. 2014. - №1.

14. Гребеньков, А. А. Киберпреследование как информационное преступление [Текст]: // Новые информационные технологии в науке нового времени: сборник статей Международной научно-практической конференции (5 октября 2016 г., Волгоград) – Уфа: АЭТЕРНА, 2016

15. ViolenceAainst Womenand Department of Justice Reauthorization Act of 2015. H.R. 3402// U.S. Government publishing Office (GPO): [Электронный ресурс]: - Режим доступа: URL: https: // www.gpo.gov/fdsys/pkg/BILLS…/pdf/bILLS-109hr3402enr.pdf /14.12.2018/. – Загл. с экрана.

16. Telecommunications and Information Technology [Электронный ресурс]: – Режим доступа: http://www.ncsl.org/research/telecommunications-and-information-technology/cyberstalking-and-cyberharassment-laws.aspx (http:// www.ncsl.org/research/telecommunications-and-information-technology/cyberstalking-and-cyberharassment-laws.aspx).- Загл. с экрана.

17. RCW 9.61.260. Cyberstalking [Электронный ресурс]: //The Revised Code of Washington.Washington State Legislature. [Электронный ресурс] URL: http:// apps.leg.wa.gov/rcw/default.aspx?cite=9.61.260. /26.08.2018/. - Загл. с экрана.

18. Шиндер, Д.Л. Киберпреступность: перед лицом проблемы [Электронный ресурс]: /Д.Л. Шиндер. – Режим доступа: www.crime-research.org. /4.06.2019./ - Загл. с экрана.

Муратбекова С.М.,
КМЮА
конституциялык жана муниципалдык укук
кафедрасынын доценти,
юридика илимдеринин доктору
Муратбекова С.М.,
доцент кафедры
конституционного и муниципального права
КГЮА, доктор юридических наук
Muratbekova S.M.,
Associate professor, Doctor of law
of Juridical sciences,
Chair of constitutional and municipal law,
Kyrgyz state academy of law
tel.: + 996 (557) 070752
e-mail: rahsalta@mail.ru

УДК347.61(575.2)

ИНТЕРНЕТ ЧӨЙРӨСҮНДӨГҮ ЖАШЫ ЖЕТЕЛЕК БАЛДАРДЫН МААЛЫМАТТЫК КООПСУЗДУГУН КАМСЫЗДООНУН КӨЙГӨЙЛӨРҮ

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НЕСОВЕРШЕННОЛЕТНИХ В СЕТИ ИНТЕРНЕТ

PROBLEMS OF ENSURING INFORMATION SECURITY OF MINORS ON THE INTERNET

Аннотация: *Илимий макалада Кыргыз Республикасында үй-бүлөө институтунун маалыматтык коопсуздугун камсыз кылуунун көйгөйлөрү, ошондой эле маалыматтык коопсуздуктун көйгөйлөргүн чечүү жолдору белгиленген.*

Аннотация: *В данной статье рассматриваются вопросы, связанные с обеспечением информационной безопасности института семьи в Кыргызской Республике, а также исследуются проблемы их обеспечения и определены пути их решения.*

Annotation: *This article discusses issues related to the information security of the institution of the family in the Kyrgyz Republic, as well as the national prerequisites for their provision. The object of consideration was also the problem of information security, identified ways to solve them.*

Негизги сөздөр: *үй-бүлөө; жашы жете элек балдар; коопсуздук; улуттук коопсуздук; маа-*