Рысмендеев Б.Дж.,
КМЮА нын ректору,
юридика илимдеринин доктору, профессор
Рысмендеев Б.Дж.,
ректор КГЮА, д.ю.н., профессор
моб. т.: +996 (772) 682711
e - mail: bakit4@mail.ru
Rismendeev B.J.,
rector KSLA,
Doctor of Law, Professor

Алишева А.Б.,
Кыргыз мамлекеттик
юридикалык академиясынын
жарандык жана үй-бүлө
кафедрасынын юридика илимдеринин
кандидаты
Алишева А.Б.,
заведующая кафедрой гражданского
и семейного права КГЮА, к.ю.н.
Alisheva A.B.,
head of the civil department and
family law of the KSLA
моб. т.: +669 (555) 212555
e - mail: aliya.alisheva@gmail.com

УДК 34.09:004.056

ИНТЕРНЕТТЕ ТЕРС МААЛЫМАТТАРДЫН ТАРАШЫ МЕНЕН КҮРӨШҮ ЖАНА АНЫН ЫКМАЛАРЫ

О НЕГАТИВНОЙ ИНФОРМАЦИИ В ИНТЕРНЕТ И МЕТОДЫ БОРЬБЫ С ЕЕ РАСПРОСТРАНЕНИЕМ

ON NEGATIVE INFORMATION ON THE INTERNET AND METHODS OF STRUGGLE AGAINST ITS DISTRIBUTION

Аннотация: *В статье проанализирована борьба в Кыргызстане и в зарубежных странах с негативной информацией в сети Интернет. Рассматривается какая разработана норматив-но-правовая база, какие методы и способы используются для обеспечения сохранности и чисто-ты виртуальной информационной среды.*

Аннотация: *Макалада Кыргызстандагы жана башка өлкөлөрдөгү Интернет түюнүндөгү терс маалымат менен күрөш анализденген. Кандай укуктук база иштелип чык-кан, маалымат-тык чөйрөнү коопсуздугун жана тазалыгын камсыз кылуу үчүн кандай ме-тоддор жана ыкма-лар иштелип чыккандыгы иликтенет.*

Annotation: *The article analyzes the struggle in Kyrgyzstan and in foreign countries with negative information on the Internet. What kind of regulatory framework is developed, what meth-ods and methods are used to ensure the safety and purity of the virtual information environment*

Ключевые слова: *Интернет, негативная информация, запрещенная для распростране-ния информация, признаки вредной информации, опыт зарубежных стран в области защиты и ох-раны граждан от вредной информации, субъектов информационного обмена, борьба с вредной информацией в сети Интернет.*

Негизги сөздөр: *Интернет, терс маалымат, жайылтууга тыюу салынган маалымат-тар, зыяндуу маалыматтардын көрсөткүчтөрү, чет өлкөлөрдө жарандарды коргоо жана коопсуздугун камсыз кылган чөйрөсүндө зыяндуу маалыматтардан жайылтууга тыюу салган тажрыйбалар, маалымат алмашуу субъекттери, Интернетте зыяндуу маалымат менен күрөшүү.*

Keywords: *Internet, negative information, information prohibited for distribution, signs of harmful information, experience of foreign countries in the field of protection and protection of citi-zens from harmful information, subjects of information exchange, the fight against harmful infor-mation on the Internet.*

Беспрепятственный доступ к ресурсам Интернет и неограниченная возможность пополнения его контента разнообразными по содержанию информацией, допускает вероятность размещения материалов незаконного характера. Перечень такой информации содержится в Гражданском кодексе КР, Законе КР «О средствах массовой информации» (ст.23) и др.

Запрещенная для распространения информация содержит определенные угрозы для личности, общества и государства. В научно-практических исследованиях предлагается введение термина «вредная информация». В ряде работ, выделяются ее характерные черты, осуществляется их классификация. Так, например, В.С. Маурин предлагает выделять следующие признаки вредной информации:

- «распространение (предоставление) ложной (неполной, искаженной) информации;
- угроза причинения (причинение) вреда жизни, здоровью, иным интересам;
- информационно-психологическое воздействие (с целью стимулирования определенного типа поведения)» [1].

В качестве определения «вредной информации», Н.Н. Ковалева предлагает формулировку следующего содержания: «информация, не являющаяся конфиденциальной, но обуславливающая необходимость охраны и защиты прав и законных интересов личности, общества и государства в силу возникновения вреда, который нанесет этим субъектам ее распространение» [2, с.108].

В этой связи интерес представляет опыт зарубежных государств в борьбе с негатив-ной информацией в сети Интернет: какая разработана нормативно-правовая база у них, какие методы и способы они используют для обеспечения сохранности и «чистоты» виртуальной информационной среды.

Итак, рассмотрим опыт Соединенных Штатов Америки с области защиты и охраны граждан от негативной, вредной информации в киберпространстве. Прежде всего, следует отметить, что Америка идет по пути абсолютной свободы выбора пользователя в отношении доступа или ограничения в доступе к той или иной категории Интернет-ресурсов. Поддержка свободы слова исходит со стороны государства. Регулирование контента со стороны Интернет-сервис провайдеров не предусматривается. Пользователь вправе самостоятельно принимать решение о доступе к той или иной информации.

Интернет провайдеры по собственной инициативе обеспечивают лишь защиту пользователей от спама и программ-вирусов. И в этой связи, они наделены полномочиями отключать тех, которые являются источниками рассылки вредоносных программ или же спама.

Что же касается наиболее уязвимой категории пользователей - детей, то защита их от негативного Интернет-контента производится путем установления специальных программ фильтров непосредственно на компьютерах в школах, библиотеках, иных образовательных учреждениях, а также по желанию родителей или опекунов, дома. Более того, вышеупомянутые образовательные заведения, а также иные государственные органы, получающие дотацию от государства, обязаны принимать меры по фильтрации информации порнографического характера, разжигающей межнациональную рознь, вызывающие расовую дискриминацию, о насилии и жестокости и т.д. [3].

Несколько иной подход используется преимущественно в странах Европы и Австралии. В этих странах применяется со-регулирование вопросов фильтрации [4].

Основной принцип, которым руководствуются при определении категорий информации, доступ к которой подлежит ограничению – сотрудничество. Правительство и Интернет-сервис провайдеры совместно решают и разрабатывают критерии для фильтруемой информации.

При этом обязанность по осуществлению этого процесса лежит непосредственно на компаниях-операторах, предоставляющих доступ к Интернет.

Особое значение придается принципу гласности: пользователей уведомляют о том, когда и по каким причинам провайдер закрывает доступ к тем или иным веб-сайтам.

В некоторых других странах, таких как Китайская Народная Республика, Корейская Народно-Демократическая Республика, Исламская Республика Иран и некоторые иные, используется жесткий контроль со стороны государства над вопросами фильтрации [5]. Правительство перечисленных стран обязывает Интернет-сервис провайдеров осуществлять цензуру Интернет контента. Сама методика фильтрации основана на использовании ключевых слов, «черных» списков веб-ресурсов, также возможно блокирование на уровне запросов в системах поисковиках. Достаточно часто доступ закрыт к новостным сайтам, официальным сайтам правительств иностранных государств. Многие веб-ресурсы, посвященные политике, развлечениям и другим подобным по содержанию, зачастую недоступны для просмотра в этих странах [6].

За нарушение и попытку «обхода» таких ограничений высока вероятность применения санкций, таких как отключение пользователей, попытавшихся обратиться к запрещенному веб-ресурсу, и также арест правонарушителей.

Что же касается практики в вопросах обеспечения информационной безопасности в сети Интернет в странах Содружества Независимых Государств, то следует сказать, что в них отсутствуют четкие правила и принципы в отношении фильтрации контента. И в этом вопросе Интернет-сервис провайдеры независимы.

Как правило, пользователь не осведомлен о том, какая информация фильтруется провайдером, по каким критериям и причинам. Этот процесс проходит не официально и гласности, как таковой, нет [7, с. 133-137]. В различных организациях довольно часто системные администраторы самостоятельно устанавливают программы-фильтры от вирусов и спама, а также ограничивающие доступ к сайтам порнографического характера, содержащим интерактивные игры и т.п.

Обоснование фильтрации Интернет-контента в интересах обеспечения национальной безопасности также не является наилучшим, поскольку дает повод для широкого толкования понятия «национальная безопасность».

Данный подход открывает возможность для необоснованного правительственного контроля над деятельностью Интернет провайдеров, как способ оправдания установления государственной цензуры и контроля.

Хотелось бы также обратить внимание на то, что возможность тотального контроля над Интернетом со стороны какого-то одного государства представляется лишь гипотетической. В то время пока одни разрабатывают способы и программы «зафильтровать» Интернет, устанавливают барьеры для доступа к той или иной категории информационных веб-ресурсов, другие занимаются созданием и поиском «обходных» программ, для преодоления данного препятствия. И свидетельством тому могут служить разнообразные программы, позволяющие миновать «барьеры» фильтрации в сети Интернет. Не обладая специальными знаниями в области информационных технологий, можно провести собственный эксперимент и убедиться в том, насколько легко можно найти некоторые из таких программ, лишь отправив запрос об этом в любой поисковой Интернет-системе. Итак, в результате совершения не сложных манипуляций, получены адреса сайтов, где подробно описывается алгоритм действий по взлому установленных фильтров [8], [9]

Хотя, с другой стороны, это вовсе не означает, что государство должно оставаться безучастным к теме защиты информационного пространства, пусть и такого специфичного как Интернет. Для этого необходимо будет участие всего международного сообщества.

А пока общего решения нет, Интернет сообщество самостоятельно пытается бороться с вредной информацией в сети Интернет (что называется саморегулированием сферы Интернет), создавая специальные сайты «санитары», «контролеры».

На этот счет можно привести конкретный пример - существует инициатива, получившая название «WOT» («Web of Trust») [10] – это бесплатная надстройка к браузеру, которая предупреждает Интернет пользователя о потенциально небезопасных веб-страницах [11]. Они работают по принципу «жалобной книги»: пользователи самостоятельно сообщают о том или ином сайте, который либо содержит информацию непристойного характера, либо является зараженным

вирусной программой, либо по иной причине является опасным. Сами-ми пользователями он помечается как «не рекомендуемый к просмотру». Как только другой пользователь попытается открыть такой сайт, он тут же будет об этом предупрежден. Однако и такой подход не является полностью универсальным, т.к. не может в полной мере обеспечить безопасность информационного пространства в сети Интернет, особенно, если речь идет о детях.

В настоящее время в Жогорку Кенеше предлагают принять закон о «Защите детей от информации, причиняющей вред их здоровью или развитию». Аналогичный документ парламентарии хотели принять еще ранее в 2012 году.

Тогда против него выступали правозащитники, операторы связи и некоторые крупные сайты, к примеру namba.kg. Противники законопроекта говорили, что, в случае его принятия, власти смогут использовать его как инструмент для цензуры [12].

Тогда в Интернете начали сбор подписей под петицией против принятия законопроекта. Под ней подписалось более тысячи пользователей.

Законопроект обязывает ставить знак возрастного ограничения для информации на телевидении, радио и в интернете, которая причиняет вред здоровью или развитию детей.

Запрещенной для детей может оказаться информация, побуждающая к насилию, употреблению наркотиков и занятию проституцией, а также содержащая сексуальные сцены, оправдания нарушения законов или дискредитации семейных ценностей.

Контент в интернете, запрещенный для детей, должен фильтроваться провайдерами связи с помощью «программно-аппаратных средств». Согласно законопроекту, процедуру фильтрации будет разрабатывать некий «уполномоченный орган».

В 2009 году предпринималась попытка принять новый закон «О государственных секретах» [13, с.33]. Однако он вызвал критику в медиа сообществе, поскольку предусматривал расширенный перечень информации, подлежащей засекречиванию, что не свойственно многим странам мира. В итоге, проект закона так и не был принят.

В 2017 году был принят Закон КР «О защите государственных секретов Кыргызской Республики». Данный Закон регулирует правовые и организационные основы отнесения сведений к государственным секретам, системы их защиты, отношения, связанные с засекречиванием и рассекречиванием таких сведений, а также иной деятельности в сфере государственных секретов в интересах национальной безопасности. В нем закрепляется, что обеспечение защиты государственных секретов осуществляют в пределах своей компетенции:

1) уполномоченный государственный орган, ведающий вопросами национальной без-опасности;

2) самостоятельное структурное подразделение (ответственное лицо) по защите государственных секретов государственных органов, органов местного самоуправления и организаций;

3) Координационный совет по вопросам защиты государственных секретов Кыргызской Республики.

Вышеуказанные субъекты, обеспечивают защиту сведений, составляющих государственные секреты, в соответствии с возложенными на них задачами и в пределах своей компетенции. Ответственность за организацию защиты сведений, составляющих государственные секреты, в государственных органах, органах местного самоуправления и организациях возлагается на их руководителей. В зависимости от объема работ с использованием сведений, составляющих государственные секреты, руководителями государственных органов, органов местного самоуправления и организаций создаются структурные подразделения (определяется ответственное лицо) по защите государственных секретов, функции которых определяются указанными руководителями с учетом специфики проводимых ими работ.

При отсутствии четкости в данной сфере возникают неоднозначные ситуации. Подтверждает это практический пример, который имел место в июне 2011 года, когда Жогорку Кенеш Кыргызской Республики принял постановление о расследовании событий апреля-июня 2010 года. Одним из пунктов постановления была блокировка издания «Фергана.ру» [14].

Хотя, у Жогорку Кенеш Кыргызской Республики нет таких полномочий.

Данная ситуация свидетельствует о возможных коллизиях при решении вопроса по ограничению доступа к информации, размещенной в сети Интернет. С одной стороны, принимать меры

необходимо своевременно. С другой – ожидание решения суда может затянуться, но, вместе с тем, характер содержания материала, попавшего под сомнение, не изменит-ся. А соответственно потенциальная угроза остается. Необходимо адекватное решение.

По нашему мнению, метод саморегулирования, раскрытый выше, является эффективным. Но не стоит недооценивать негативные стороны. Существует вероятность, что может быть попытка преднамеренного устранения конкурентов в сети Интернет. То есть, специально «забанить» (от англ.слова «ban» - запрет) «определенный сайт, путем навешивания на не-го ярлыка будто он «может содержать вредоносные вирусы» (т.е. перед пользователем при нажатии на ссылку с необходимым для него сайтом, появится предупреждение, о том, что этот ресурс может нанести вред компьютеру, с рекомендацией не открывать его). Соответственно, такого характера предупреждение может испугать потенциального посетителя сайта, что, в последующем, может отразиться на экономической составляющей.

Хотя, технологию предупреждения в сети Интернет о «неправомерном» контенте можно взять на вооружение. В частности, как было установлено в ходе исследования, ограничение доступа к информационным ресурсам в сети Интернет возможно лишь на основании вступившего в силу решения суда о признании того или иного материала «вредным» по со-держанию.

Но зачастую, судебное разбирательство затягивается, а материал, содержащий противозаконную информацию, остается в свободном доступе. Учитывая мгновенность распространения информации посредством сети Интернет, можно утверждать, что после принятия решения судом о характере информации (в том случае, если будет установлено, что она является «вредной» по содержанию) уже будет неактуальным.

В условиях информационного общества, считаем, что меры по обеспечению общественной безопасности должны приниматься своевременно. В этой связи, предлагаем в пери-од рассмотрения судебного дела и до вынесения по нему решения, применять технические меры к Интернет-странице, на которой размещена информация спорного характера. Так, по ходатайству заявителя, адвоката, прокурора, на основании определения суда приостанавливать распространение информации и ограничивать доступ к соответствующему материалу на сайте. Такие меры могут быть выражены в форме всплывающего «окна» с предупреждением пользователя о возможном «вредном» содержании материала при обращении запроса в сети Интернет к Интернет-странице с данной информацией. Причем, в этом «окне» должно быть указано:

- основание ограничения доступа,

- дата начала применения меры по ограничению доступа, и инстанция, в которой про-ходит разбирательство по данному делу.

Но, при этом, сам материал может и не быть удален, пока не определится его судьба, но ознакомление с ним, его просмотр, загрузка и т.д. будет невозможными. Безусловно, при наличии желания можно получить доступ к «сомнительной» информации, используя специальные программы. Но, все же, для этого необходимо будет предпринять определенные действия, что может повлиять на снижение количества посещений пользователей на конкретную Интернет-страницу.

Хотелось бы обратить внимание, что предлагается ограничить доступ именно к конкретной Интернет-странице, на которой размещен «спорный материал», но не ко всему сайту.

Следует отметить, что особенно актуальны в последнее время вопросы защиты личных прав граждан, нарушаемых посредством сети Интернет. В частности, право на честь, достоинство и деловую репутацию, право на охрану тайны личной жизни, право на собственное изображение, право на защиту персональных данных и иных правах.

Безнаказанное размещение компрометирующих материалов превратило Интернет в источник повышенной опасности. Так, Интернет используется для дискредитации общественных деятелей, чиновников различных рангов, конкурентов в избирательных кампаниях, да и простых граждан.

Оклеветать или опорочить честь, достоинство персоны в настоящее время не составляет труда: можно лишь разместить информационный материал о нем необходимого содержания в сети Интернет на популярном сайте. И, можно быть уверенным, что множество пользователей ознакомятся с его содержанием, возможно, даже распространят его дальше на других сайтах, перепечатают в газетах, журналах, осветят через вещательные каналы. Т.е. гарантировано довести

до сведения неограниченному кругу лиц ту информацию, которая требуется для поднятия его рейтинга или для его снижения.

Не все «обиженные» личности обратятся в суд, поскольку это связано с прохождением определенных процедур. Да и не всегда суды с легкостью могут выносить решения по спорам, связанных с подобными случаями. Сложность заключается в том, что достаточно затруднительно определить круг виновных лиц. Одно из преимуществ Интернет – анонимность – может стать его негативной характеристикой. К тому же, не всегда просто обеспечить доказательственную базу нарушенного права. Особенно это отягащается при наличии иностранного элемента – а это абсолютно естественно для Интернет.

Субъектов информационного обмена, распространяющих порочащие и компрометирующие сведения, находящихся на территории Кыргызстана, можно хоть как-то выявить. Однако, учитывая отсутствие жесткой привязки к территории Интернет и сложного правового определения понятий «кыргызский сегмент», есть вероятность, что компрометирующий материал может быть размещен на сервере другой страны.

Учитывая сложность и длительность процессуальной процедуры исполнения между-народных поручений, для скорейшего пресечения распространения компромата можно было бы также применить технические меры по ограничению к нему доступа, предложенные выше.

Актуальной была бы разработка и проведение учебных семинаров для подготовки су-дейского корпуса по проблемам, затрагивающим Интернет сферу. Не лишней была бы для них информация об устройстве Интернет, его специфических свойствах, о возможностях фиксации факта присутствия в сети под определенным IP-адресом, а также о техническом потенциале оборудования, обслуживающего сеть Интернет с тем, чтобы владеть информацией о том, какие документы и от кого могут быть судом истребованы для обеспечения доказательственной базы.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. Маурин, В.С. Правовой анализ вредной информации в условиях информационного общества [Электронный ресурс]: автореф. дис. … канд. ист. наук: 12.00.14 / В.С. Маурин. - М., 2004. – 190 с. - Режим доступа: http://www.dissercat.com/content/pravovoi-analiz-vrednoi-informatsii-v-usloviyakh-informatsionnogo-obshchestva. – Загл. с экрана

2. Средства массовой информации и право в Кыргызской Республике [Текст]: учеб. для вузов / К.К. Керезбеков, Ч.А. Мусабекова, Г.Т. Искакова, Э.А. Кочкарова //Под общ.ред. Ч.А. Мусабековой. – Б., 2002. – 272 с.

3. Regardless of Frontiers, Protecting the Human Right to Freedom of Expression on the Global Internet [Электронный ресурс]: - Режим доступа: http://www.cdt.org/gilc/report.html – Загл. с экрана.

4. Беспалов, Е.И. Интернет-политика разных государств мира [Электронный ресурс]: - Режим доступа: www.hitechno.ru/?page=event9. – Загл. с экрана.

5. Доклад Организации по безопасности и сотрудничеству в Европе «Контроль над Интернетом» [Электронный ресурс]: - Режим доступа: http://news.ntv.ru/97303/, http://www.utro.ru//news/2007/07/29/667037.shtml и др. – Загл. с экрана.

6. Новые ограничения на Интернет в Китае [Электронный ресурс]: - Режим доступа: http://www.computerra.ru/focus/new/19203/. – Загл. с экрана.

7. Pluralism in the media and Internet [Текст]: / Colin Guard. Observation on Internet Free-dom and Development in Eleven Countries of Eurasia (Office of Representative on Freedom of the Media Organization for Security and Co-operation in Europe: Vienna, 2006), - p.133-137.

8. Обход интернет-фильтров [Электронный ресурс] - Режим доступа: http://www.computerra.ru/gid/rtfm/internet/331592/. – Загл. с экрана.

9. Достучаться до Небес, или Как получить доступ к сайтам [Электронный ресурс]: - Режим доступа: http://magazeta.com/psi/2007/12/09/knockin-on-heavens-door/. – Загл. с экрана.

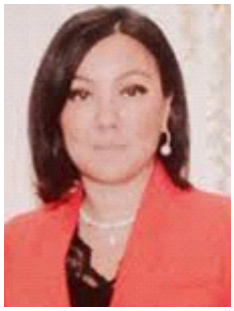
10. Community-powered tools that boost trust on the web [Электронный ресурс] - Режим доступа: http://www.mywot.com/en/scorecard – Загл. с экрана.

11. WOT: Web of Trust [Электронный ресурс]: - Режим доступа: http://www.ru.wikipedia.org/wiki/WOT:_Web_of_Trust. – Загл. с экрана.

12. Парламент опять предложил защищать детей от «вредной» информации в интер-нете. Законопроект очень похож на российский [Электронный ресурс]: - Режим доступа: https://kloop.kg/blog/2019/02/27/parlament-opyat-predlozhil-zashhishhat-detej-ot-vrednoj-informatsii-v-internete-zakonoproekt-ochen-pohozh-na-rossijskij/. – Загл. с экрана.

13. Алагушев, А.К. Алишева, Н.И. Правовая среда для развития и деятельности СМИ в Кыргызской Республике [Текст]: /А.К. Алагушев, Н.И. Алишева - Б., 2010 – С. 33.

14. В Кыргызстане начался судебный процесс по блокировке интернет-сайта между-народного информационного агентства «Фергана» [Электронный ресурс]: - Режим доступа: http://www.24kg.org/reportaji/143700-missiya-vosstanovit-spravedlivost.html. – Загл. с экрана.



Сабитова А.А.,
Абай атындагы КАЗУПУнун
Сорбонна-Казакстан Институтунун директору,
юридика илимдеринин доктору, профессор
Сабитова А.А.,
доктор юридических наук, профессор
директор Института Сорбонна-Казахстан
КазНПУ имени Абая
г. Алматы
Ainur Sabitova
Directrice de l'Institut Sorbonne-Kazakhstan
L'Université Kazakhe Nationale Pédagogique Abaï
Almaty, Kazakhstan

УДК 340.130.53(9)-061.3

ТЫНЧТЫК ЖЫЙНАЛЫШ УКУГУ БОЮНЧА: ЭЛ АРАЛЫК УКУК АСПЕКТИСИ

О ПРАВЕ НА МИРНЫЕ СОБРАНИЯ: МЕЖДУНАРОДНО-ПРАВОВЫЕ АСПЕК-ТЫ

SUR LE DROIT DE LA REUNION PACIFIQUE

Аннотация: *Эл аралык укуктун аспектилери боюнча тынчтык жыйналышын өткөрүү укуктары каралат. Дүйнөдө болуп жаткан өзгөрүүлөрдүн шартында мамлекеттик ички жөнгө салуу чөйрөсүнөн адамдын укутары жана эркиндиктери эл аралык укуктун жаңы багытына фактылык жана юридикалык түрдө белгиленген. Мамлекеттин ички жана эл аралык укуктарды бириктирүү актүвдүү жүрүп жатат. Азыркы күндө көп мамлекеттер-де конституциялык-укуктуктун ичинен башкаруу жыйналыш укугунун эркиндиги жети-шерлик деңгээлде иштелген эмес деп белгилейт автор.*

Аннотация*: В статье рассматриваются международно – правовые аспекты на реализацию права на мирные собрания. Приводится анализ международно-правовой регламентации*