УДК 327 (470+571):327,5

Амедов Джемиль Назимович, аспирант Гуманитарно-педагогическая академия (филиал) ФГАОУ ВО «Крымский федеральный университет имени В.И. Вернадского» в г. Ялте

e-mail: powell_9_74@mail.ru

КИБЕРТЕРРОРИЗМ КАК НОВАЯ УГРОЗА МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

Аннотация. Российские представления о природе, потенциале и использовании киберпространства значительно отличаются от западного. У России есть особенное глубокое беспокойство по поводу принципа безудержного обмена информацией в киберпространстве, и предположение, что национальные границы имеют ограниченную уместность в этом пространстве. Круговорот информации, которая представляет собой угрозу обществу или государству и суверенитету «национального Интернета», является ключевыми проблемами безопасности в России.

Это расхождение подрывает попытки достигнуть соглашения по общим принципам и правилам поведения для киберпространства с Россией, несмотря на повторные российские попытки представить нормы подобного типа и призывы к другим государствам поддержать данную инициативу.

Данная статья исследует аспекты двух публичных заявлений российской стороны в отношении киберпространства: «Проект конвенции по Международной информационной безопасности» от 24 сентября 2011 года и российская военная киберпервичная доктрина «Концептуальные Представления о Деятельности Вооруженных сил Российской Федерации в Информационном пространстве» от 22 декабря 2011 года, чтобы описать российскую общественную позицию по киберпространству.

Российские власти полагали, что протесты в связи с результатами

выборов Государственной думы в декабре 2011 г. возникли, по крайней мере, частично из-за кибер кампании (информационной войны) против России. Информационный и политический ответ российских властей на это событие взят в качестве тематического исследования, чтобы оценить практическое воздействие российских представлений, обрисованных в общих чертах выше.

Ключевые слова: Россия, информационная безопасность, социальные медиа, гражданский протест, политика, вооруженные силы

CYBER TERRORISM AS A NEW THREAT TO INTERNATIONAL SECURITY

Amedov Dzhemil Nazimovich, graduate student The Humanitarian Pedagogical Academy (branch) FGAOU VO "Crimean federal University named after V.I. Vernadsky "in the city of Yalta

e-mail: powell_9_74@mail.ru

Abstract. Russian views on the nature, potential and use of cyberspace differ significantly from the Western consensus. In particularRussia has deep concerns on the principle of uncontrolled exchange of information in cyberspace, and over the presumption that national borders are of limited relevance there. Circulation of information which poses a perceived threat to society or the state, and sovereignty of the «national internet», are key security concerns in Russia.

This divergence undermines attempts to reach agreement on common principles or rules of behaviour for cyberspace with Russia, despite repeated Russian attempts to present norms of this kind to which other states are invited to subscribe.

This paper examines aspects of the two most recently released public statements of Russian policy on cyberspace: the «Draft Convention on International Information Security» (released 24 September 2011) and the Russian military cyber proto-doctrine «Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space» (released 22 December 2011) in order to describe the Russian public stance on cyberspace.

The Russian authorities considered that protests over the State Duma election results in December 2011 arose at least in part because of a cyber/information warfare campaign against Russia. The informational and political response of the Russian authorities to this is taken as a case study to measure the practical impact of the Russian views outlined above.

Keywords: Russia, information security, social media, civil protest, policy, military.

Внешним наблюдателям диалог между Россией и Западными партнерами по проблемам киберпространства кажется характеризуемым взаимным непониманием и очевидной непримиримостью. Нормы, которые считаются само собой разумеющимся на одной стороне, рассматриваются как угроза другими, и отсутствие общего словаря или общих понятий, касающихся киберпространства, означает, что даже когда предприняты попытки для поиска точек соприкосновения, то и они скоро терпят неудачу.

По словам Министра связи и массовых коммуникаций России Игоря Щеголева «в настоящее время, на Западе не все всегда понимают то, каким правилам мы следуем» [1]. Это остается верным несмотря на то, что Россия уже больше десятилетия пытается собрать международную поддержку для этих правил во множестве международных форумов, включая Организацию Объединенных Наций [2] и многие другие [3]. В данной статье рассматриваются два публичных заявления российского подхода к информационной безопасности для описания ключевых принципов российского подхода.

В сентябре 2011 г. в Екатеринбурге на Международной встрече высокопоставленных должностных лиц, ответственных за вопросы безопасности был опубликован «Проект Конвенции по международной информационной безопасности», который практически повторял «Международные нормы поведения для информационной безопасности», представленные Россией и другими государствами в Организации

Объединенных Наций [4].

Ключевые положения документа были сжаты в список из 23 основных проблем беспокойства России в информационном пространстве Институтом информационных вопросов безопасности (ИИВБ) Московского государственного университета, который занимался разработкой данного проекта Конвенции. Эти проблемы, каждая из которых отражена в одной или нескольких статьях предложенного документа, включают некоторые условия, которые не должны вызывать противоречий ни у одной из стран-участниц, такие как предотвращение нарушений прав и свобод, или «криминализации использования информационных ресурсов в незаконных целях».

Но в то же время, множество проблем было связано с противоречиями о представлениях об использовании и управлении Интернетом, которые появились в США, Великобритании и других аналогично мыслящих государствах. Это система взглядов, которая формирует неофициальное и нигле незакрепленное согласие - упомянутое далее, для краткости и ясности, как «Западное согласие». Так это «согласие» отражено во многих изданных международных документах, например, в рекомендациях Организации экономического сотрудничества и развития (ОЭСР) об основах Интернет-политики [5].

Следует отметить, что ключевым расхождением между российскими и западными подходами к кибербезопасности – это восприятие содержания самого термина «угроза» [6]. В российском понимании он определен как «угроза использования содержания для влияния на социально-гуманитарную сферу». В отличие от этого, Западное согласие признает угрозу от враждебного влияния, но обычно обесценивает проблему враждебного содержания. Рекомендации ОЭСР, упомянутые выше, например, включают «свободный поток информации и знаний, свободу самовыражения, ассоциации и собрания, защиту свобод личности, как критические компоненты демократического общества и культурного разнообразия» [5].

Это регулярно отмечается как основной принцип, «что

киберпространство остается открытым для инноваций и свободного потока идей, информации и выражения», как указано британским министром иностранных дел Уильямом Хэйгом и другими западными представителями на Лондонской конференции [7]. В то же время на той же самой конференции, российский Министр связи и массовых коммуникаций Игорь Щеголев подверг критике принцип свободного потока информации: это должно регулироваться и национальным законодательством, и контртеррористическими соображениями - связанными с другим принципом в списке, «ограничения прав и свобод только в интересах безопасности» [8].

Таким образом, в то время как обе стороны публично поддерживают свободу обмена информацией, и таким образом иногда создают иллюзию согласия, на самом же деле расширение действия применения данного принципа весьма затруднительно в связи с тем, что на практике взгляды сторон так же далеки друг от друга.

Две последующие проблемы были определены ИИВБ как «Воздержание от использования информационно-коммуникационных технологий для вмешательства в дела других государств» и «Угрозы использования доминирующего положения в киберпространстве» на основании высказывания определенными структурами российского руководства, что протестные движения, последовавшие за парламентскими выборами в декабре 2011 года были вдохновлены и финансированы из-за границы. В частности, упоминание о «доминирующем положении в киберпространстве» относится к идее «информационного пространства, являющегося местом соревнования по информационным ресурсам... США в настоящее время - единственная страна, обладающая информационным превосходством и способностью значительно управлять этим пространством» [9].

Однако принцип неделимости безопасности подчеркнут и в проекте Конвенции. Здесь снова, очевидное согласие скрывает принципиальное разногласие – просто потому, что у этой общей фразы есть совершенно различные значения на русском и английском языках. Несмотря на признание и

терпеливое объяснение, что использование идентичных фраз, относящихся к сильно разнящимся понятиям приводит к недоразумению и недопониманию [10], данные аспекты продолжают рождаться и в Западной и в российской риторике, что затрудняет диалог, зачастую превращая его в выражение «каждый понимает все по-своему» [11].

«Интернет-суверенитет» является другой ключевой областью разногласия. Россия, наряду со многими аналогично мыслящими странами (например, страны члены СНГ), поддерживает идею национального контроля всех Интернет-ресурсов, которые лежат в пределах физических границ государства и связанного понятия применения местного законодательства, или, как сформулировано в проекте Конвенции, «каждое государство-член наделено правом сформулировать суверенные нормы и управлять его информационным пространством согласно его внутригосударственным законам» (Статья 5.5).

Это находится в прямой оппозиции к подходу, провозглашаемому США. Так госсекретарь США Хиллари Клинтон в декабре 2011 г., заявила, что такие страны, как Россия, хотели «уполномочить каждое отдельное правительство делать свои собственные правила для Интернета, которые не только подрывают права человека и свободный поток информации, но также и совместимость сети. В действительности правительства, выдвигающие такую повестку дня, хотят создать национальные барьеры в киберпространстве. Этот подход имел бы катастрофические последствия для Интернет-свободы» [12].

Список основных принципов, обеспеченных ИИВБ, включает и «Принятие существенных мер для предотвращения разрушительной информационной деятельности от территории под юрисдикцией государства». Это относится и к разделу в проекте Конвенции, который касается государств, гарантирующих, что информационная инфраструктура в их собственной юрисдикции не используется для враждебной деятельности и сотрудничества, чтобы определить источник такой деятельности (Статья 6.2). Рассмотрение практических последствий соглашения этого вида и обязательства, которые оно влечет за собой, быстро приводят к реализации огромного законодательного и

административного бремени на государства, которые хотели бы подписаться под проектом данной Конвенции. Мало того, что они должны контролировать законность содержания в их собственной юрисдикции, но также и гарантировать, что это считают безобидным и невраждебным в юрисдикции всех других подписавшихся - иначе, они могут немедленно быть обвинены в разрешении враждебной деятельности в нарушении Конвенции.

Другое ключевое условие, которое носит в себе недопонимание это «принятие мер юридической или другой природы … к определенным частям информации и коммуникационной инфраструктуре государства-участника». В тексте проекта Конвенции это звучит как «исполнение необходимых шагов законодательной или другой природы, которая гарантирует законный доступ к определенным частям информации и коммуникационной инфраструктуре на территории государства-участника, которые по закону вовлечены в то, чтобы быть используемым для предотвращения террористической деятельности в информационном пространстве» (Статья 9.5).

Две важных области концептуального расхождения возникают здесь: во-первых, упоминание о «терроризме», и во-вторых, проблема доступа к информационному пространству иностранного государства.

Данные концептуальные различия в понимании природы «терроризма» между российским и западными государствами, обеспечивают дополнительные сложности и неопределенности к пониманию того, что составляет «кибертерроризм». Как описано Анной-Марией Тэлихарм, Алексом Майклом и другими исследователями, «есть большое изобилие различных определений идеи терроризма..., добавление префикса «кибер» только расширило список возможных определений и объяснений» [13, 14].

Таким образом, без согласия с Россией о том, что скрывается за «преступлением террористической деятельности в информационном пространстве», этот пункт остается неразрешенным. Такое согласие вряд ли будет достигнуто, учитывая фундаментальные и нерешенные различия между Москвой и Западом касаемо того, что составляет терроризм и

контртеррористическую деятельность [15].

В то же время призыв к санкционированному доступу к информационной инфраструктуре в юрисдикции другого государства напоминает текст статьи 32 Конвенции Совета Европы по киберпреступности (Будапештское соглашение): «Сторона может, без разрешения другой Стороны... иметь доступ или получать, через компьютерную систему на ее территории, сохраненные компьютерные данные, расположенные в другой Стороне, если Сторона получает законное и добровольное согласие человека, у которого есть законные полномочия раскрыть данные Стороне через ту компьютерную систему» [16].

Этот текст составляет главное возражение России на ратификацию Будапештского соглашения [17]. Ключевая фраза, которая вызывает российское возражения – это «без разрешения другой Стороны». Согласно российским представлениям, это неприемлемое нарушение принципа суверенитета. Кроме того, диапазон вариантов, скрытых за «человеком, у которого есть законные полномочия раскрыть данные», является источником беспокойства, поскольку это могут быть организации, отличные от государства. Российские опасения по поводу практического применения Будапештского соглашения иллюстрированы отчетом в «Российской газете», которая подчеркнула «сомнительное предоставление для иностранных спецслужбдля вторжения в наше киберпространство и проведение их специальных операцийбез уведомления наших разведывательных служб» [18].

Однако в целом, статьи проекта Конвенции и его основные принципы служат тому, чтобы иллюстрировать два появляющихся согласия по управлению Интернетом. Первое заключается в том, что в Западном понимании, настаивающем на свободном и неограниченном потоке информации, в Интернете присутствуют информационные потоки, которыми не управляют. И второе - в отношении Конвенции, поддержанной Россией и другими государствами, с важными замечаниями о потоке информации и необходимости государственного суверенитета в киберпространстве.

Новым официальным российским программным заявлением о

киберпроблемах, является «Концептуальные взгляды о деятельности Вооруженных сил Российской Федерации в информационном пространстве» (далее – Взгляды). Этот документ был представлен на информационной конференции по безопасности в Берлине 14 декабря 2011 года [19] и опубликован в текстовой форме 22 декабря 2011 года [20].

Несмотря на большой объем предыдущей полуофициальной литературы по информационной войне, это - первое явное публичное заявление роли российских вооруженных сил в киберпространстве, которое можно расценивать как первичная российская военная кибердоктрина. В сравнении с аналогичными документами, опубликованными в США, Великобритании и в других странах, весьма интересно, что она в себя включает и чем явно пренебрегает.

Это определенно российский документ, который не похож на аналогичные иностранные, например, американскую Стратегию работы в киберпространстве Министерства обороныСША [21] не только через ссылки на поддержку относящихся к доктрине документов (Военная доктрина и информационная Доктрина безопасности Российской Федерации), но и в ее основных предположениях и определениях информационных проблем.

Таким образом, это подтверждает давнее признание того, что потенциальные операции в информационном пространстве создают совершенно новый набор проблем [22]. Вместе с тем, очевидно, что иностранное толкование информационной безопасности, наряду с другими областями военной деятельности, не применимо к российским обстоятельствам - как определно в 1995 голу выдающимся российским военным комментатором Виталием Цымбалом: «Ошибочно предполагать, что мы можем целесообразно интерпретировать и использовать для наших собственных нужд иностранные идеи об информационной войне (ИВ) и их терминологии, чтобы избежать беспорядка и недопонимания при международных обсуждениях, во время обмена информацией, или во время контакта между специалистами. Как раз наоборот, не имеет никакого смысла копировать просто любое понятие ИВ. В

понятие ИВ для Министерства обороны Российской Федерации должны быть включены конституционные требования РФ, ее основных законов, специфических особенностей существующей экономической ситуации РФ и миссий наших Вооруженных сил.

Они вторят защитной линии других российских документов, касающихся киберпространства, включая проект Конвенции, описанный выше, и цитируют в их преамбуле заявление внешней угрозы информационной безопасности России, исходящей от других государств, развивающих информационные понятия войны [6]. Далее, они заявляют, что «предназначенная система деятельности была установлена в Вооруженных силах Российской Федерации для того, чтобы предусмотреть эффективное сдерживание, предотвращение и разрешение военных конфликтов в информационном пространстве» [23].

Определение информационной войны, которую вооруженные силы призваны удержать и предотвратить, стоит процитировать полностью, поскольку это иллюстрирует устойчивую целостную природу российского восприятия информационной войны икибер-конфликта как неотъемлемой его части.

Информационная война – это «конфликт между двумя или более государствами в информационном пространстве с целью принесения убытков критически важным информационным системам, процессам и ресурсам, а также другим структурам, свержение политических, экономических и социальных систем, массовой психологической работы над населением, направленной на дестабилизацию общества и государства, и принуждение правительствапринятия решений в интересах противостоящей сторон».

Законность объявлена первым принципом, управляющим военной деятельностью. Наряду с обычными ссылками на первенство международного права и принцип невмешательства во внутренние дела других государств, Взгляды отмечают, что использование Вооруженных сил за пределами Российской Федерации подвергается процессу одобрения Федерального собрания и указывает на то, что «это предоставление должно также быть

расширено на использование Вооруженных сил Российской Федерации в информационном пространстве» (Раздел 2.1, Законность) Взгляды также даютдопуск для «развертывания сил и ресурсов дляобеспечения информационной безопасности на территориях других государств» (Раздел 3.2, Решение Конфликтов), что вынуждает прогрессивно склонных невоенных российских интернет-экспертов искаженно размышлять о картине «коммандос, спускающихся с парашютом в центры сервера, с iPad в руке».

Первоочередная задача для Вооруженных сил указана как «стремление собрать текущую и достоверную информацию относительно угроз» и разработки контрмер - но это явно в военных целях. Цель состоит в том, чтобы, прежде всего, защитить военные системы командования и управления, и «поддерживать необходимое моральное и психологическое состояние персонала». Это стало важным с тех пор как «теперь сотни миллионов людей (целые страны и континенты) вовлечены в объединенное глобальное информационное пространство, сформированное Интернетом, электронными СМИ и системами мобильной связи». То, что отсутствует, является упоминанием о военной роли в оценке или противостоянии угрозам более широкому обществу или российскому государству (Раздел 2.2., Приоритеты).

Российская военная деятельность в информационном пространстве «включает в себя оценку ситуации штабом, действия, совершенные войсками в плане разведки, эксплуатационном обмане, радиоэлектронной войне, коммуникациях, скрытом и автоматизированном командовании и контроле, информационной работой штабквартиры и защита информационных систем от радиоэлектронного, компьютерного и другого воздействия».

Также в отличие от иностранных относящихся к доктрине заявлений, Взгляды указывают на «учреждение международного правового режима», регулирующего военную деятельность в информационном пространстве как основную цель международного сотрудничества с «дружественными государствами и международными организациями». (Раздел 2.5, Сотрудничество)

Эти дружественные организации: CollectiveSecurityTreatyOrganisation (CSTO), Содружество Независимых Государств (СНГ) и ShanghaiCooperationOrganisation (SCO). Но это группы государств, которые уже сделали значительные успехи в формализации их разделенных взглядов на информационную безопасность. У CSTO есть «Программа совместных действий для создания системы информационной безопасности государств-членов CSTO» [24], в то время как SCO заключил «соглашение среди правительств государств-членов SCO о Сотрудничестве в Области Обеспечения Международной информационной безопасности» [25,6].

Но в дополнение к этому, вооруженные силы, как предполагается, «работают над созданиемс Организацией Объединенных Наций соглашения о международной информационной безопасности, расширяющей сферу компетенции классических принятых норм и принципов международного права по отношению к информационному пространству». Российские вооруженные силы, таким образом, предназначены для того, чтобы способствовать в продвижении таких инициатив как проект Конвенции по международной безопасности, что схоже с ролью большинства Западных вооруженных сил.

Этот акцент на международные юридические усилия повторяет заявления, сделанные высшими российскими военными чинами после вооруженного конфликта с Грузией в августе 2008 года. Генерал Александр Бурутин, в это время заместитель начальника Генерального штаба, сказал, что необходимо «переместиться от анализа проблем и угроз в информационной безопасности к ответу и предотвращению» [26].

Оба эти стремления отражены в«Концептуальныхвзглядах о деятельности вооруженных сил Российской Федерации в информационном пространстве» и в проекте «Конвенции по международной информационной безопасности». И оба документа, описанных выше, ссылаются, прямо или косвенно, на информационную Доктрину безопасности Российской Федерации (2000) [27].

Эта «доктрина», в российском смысле «национальной политики», является фундаментальным документом, главным подходом России к

информационной безопасности, и как составное подмножество информационной безопасности, кибер-проблем. Она содержит те же самые либеральные условия для бесплатного обмена информацией, как требуют Уильям Хэйг и Хиллари Клинтон. А сама доктрина предназначена «гарантировать конституционные права и свободы человека и гражданинадля свободногопоиска, получения, передачи, создания и распространения информации любыми законными средствами» (Статья I, Часть 1).

Доктрина предусматривает «разработку методов для увеличения эффективности государственного участия в формировании политики общественной информации вещательных компаний, других общественных СМИ» (Статья I, Часть 4). Основное понятие, отраженное в других относящихся к доктрине заявлениях, то, что СМИ - инструмент государства для формирования общественного мнения способом, благоприятным в отношении властей.

Во время выпуска информационной Доктрины безопасности генерал-полковник Владислав Шерстюк, тогда первый заместитель министра Совета безопасности Российской Федерации, ответственный за информационную безопасность и один из ключевых разработчиков документа, объяснил, что доктрина не будет использоваться, чтобы ограничить независимые СМИ, но, в то же время, все СМИ, как правительственные, так и частные, должны являться объектом государственного наблюдения [28]. В результате реакция представителей российского руководства, высказанных через независимые СМИ, была проявлена ответом тогдашнего премьер-министра России В.В. Путина к сообщению о европейских планах противоракетной обороны радиостанцией Эхо Москвы: В. Путин описал опыт слушания как «диарея, льющаяся на него днем и ночью» [29].

Таким образом, представленная доктрина указывает на то, что «основные виды деятельности в области информационной безопасности Российской Федерации в сфере внутренней политики - это усиление действий контрпропаганды, нацеленных на предотвращение отрицательных эффектов

распространения дезинформации о внутренней политике России» (Статья II, Часть 6), а также «развитие определенных правовых и институциональных механизмов, чтобы предотвратить незаконную информацию - психологические влияния на массовое сознание общества» (Часть 7 Статьи II). А способность к «предотвращению отрицательных эффектов» была проверена организацией онлайн массовых митингов протеста после выборов в российский парламент 4 декабря 2011 года.

Однако протесты и инакомыслие после парламентских выборов 2011 года стали рассматриваться как организация информационной войны против России.Вмешательство в информационные ресурсы было очевидно, однако это не дошло до полной информационной блокады, ожидаемой некоторыми аналитиками [30].

Гражданские протесты в связи с результатами выборов, возможно, упали в серую область для некоторых практиков безопасности в России между законным протестом и опасной подрывной деятельностью, приведя к смешаннойреакции, включая неэффективные попытки заблокировать оппозиционные коммуникационные и интернет-ресурсы.

Подозрение в иностранном участии вызвало страх перед подрывной деятельностью и «цветной революцией», связанное с распространяющимся аргументом, что политическая нестабильность в Северной Африке и Ближнем Востоке была следствием планов Запада во главе с США [31]. Как отметил тогдашний Президент В. Медведев Россия была уязвима для такого вида вмешательства. Говоря в феврале 2011 г., он сказал: «Посмотрите на ситуацию, которая развернулась на Ближнем Востоке и арабском мире. Это чрезвычайно плохо. Впереди главные трудности... Мы должны смотреть правде прямо в глаза. Это - сценарий, который они готовили для нас, и теперь они еще сильнее будут пытаться его реализовать» [32].

Действительно военная кампания в Ливии точно соответствовала образцу «современной войны», описанной руководителем Генерального штаба Николаем Макаровым в опубликованных статьях: «Использование

политического, экономического и информационного давления и подрывных действий, сопровождаемых развязыванием вооруженных конфликтов или местных войн, действий, которые приводят к относительно небольшому кровопролитию, для достижения намерений агрессора» [33].

Данные процессыдают начало двум ключевым проблемам: во-первых, прецедент установлен для вмешательства во внутренние дела суверенного государства с намерением смены режима; и во-вторых, риск, что вмешательство «могло непредсказуемо привести к крупномасштабной войне, вовлекающей непредвиденных противников» [33].

Совершенно иное мнение Тима Томасаоинформационных методах войны: «Дезинформация –это российская тактика, которая управляет восприятием и информацией, и дезинформирует людей или группы людей. Некоторые методы дезинформации довольно очевидны, некоторые неубедительны, другие работают посредством отложенного восприятия, слухов, повторения или аргументов. Определенные люди или конкретные социальные группы могут служить целями дезинформации... В России сегодня, где нестабильная общественно-политическая и социально-экономическая ситуация существует, все население может служить целью влияния для вражеской кампании по распространению дезинформации. Это - главный российский страх» [34].

Безусловно, этот страх дает начало еще большим несовместимостям между российским и западным подходом к интернет-свободе. На конференции по разоружению ООН в 2008 году [35], российский представитель Министерства обороны предположил, что любые правительственные идеи в Интернете с намерением свергнуть правительство другой страны во имя демократической реформыбудут характеризоваться как «агрессия» и вмешательство во внутренние дела [3]. Это,несомненно, относится и к российским предположениям о том, что иностранные СМИ способствовали и финансировали протесты после парламентских выборов в России.

В ответ на эти протесты была проведена проверка в отношениисоциальной сети Твиттер, которая использовалась в качестве

ключевого инструмента для организации митингов в течение декабря 2011 года [36, 37]. Также был совершен официальный запрос Федеральной службы безопасности России к сайту социальной сети VKontakte, чтобы заблокировать определенные страницы, организующие протесты, однако был отклонен как незаконный [38].

Как отмечено аналитиком Кимберли Зензом, разместившим на LinkedIn в январе 2012 года «нацеленность на внутренние сайты не работала, а попытки управлять содержанием на иностранных сайтах тоже не увенчались успехом, и внутренние компании (LiveJournal и затем VKontakte) также не были надежными партнерами. В действительностивариантов для государственного управления онлайн-контентом, кажется, не хватает. Это связано с широко применимым представлением, что быстрое появление протестов застало правительство врасплох и показало его неспособность понять, как степень недовольства среди населения, так и растущую мощь социальных медиа [39]».

Это еще раз подтверждает заявление секретаря Совета безопасности Российской Федерации Николая Патрушева, высказанное в статье «США скрываются позади сказок о правах человека», в которой он заметил, что определенная степень интернет-регулирования важна. «Конечно, в России должно быть разумное регулирование, так же, как это сделано в Соединенных Штатах, Китае и многих других странах», написал Патрушев [40].

Между тем Министр связи и массовых коммуникаций Игорь Щеголев отметил, что, «хотя кибербезопасность и поведение онлайн - текущие проблемы в современном мире, блокировать Интернет или ограничивать доступ к социальным сетям, недопустимо при любых обстоятельствах». «Есть мнение, что российское правительство предположительно стремится достигнуть большего государственного контроля над Интернетом. Но в России мы даже не рассматриваем возможности блокирования доступа к Твиттеру или Facebook, в то время как в некоторых европейских странах было открыто указано, что это будет сделано», подчеркнул министр [1].

Таким образом, российский ответ на онлайн инакомыслие после

декабрьских выборов не был таким драконовским, как иногда его изображают в Западных комментариях, но и не был либеральным, как предлагает поверхностное чтение российских программных документов. Россия продолжает стремиться к международным соглашениям, регулирующим киберпространство в виде согласия, уже достигнутого с государствами, придерживающимися российского курса в интернет-безопасности, в CSTO и SCO. Но проблема Западных стран, стремящегося сотрудничать с Россией по этим вопросам, состоит в том, чтобы понять, что включает в себя само понятие «кибертерроризм». Фундаментальные положения, определенные российским подходом в решении этого вопроса, очень отличаются от Западного и во многих случаях, внешне схожие трактовки, используемые двумя сторонами, служит лишь тому, чтобы замаскировать эти различия.

Список источников:

1. Интерфакс, “Щеголев: цензуры интернета в России не допустят,” 20 января 2011 г. [Электронный ресурс]. Режим доступа: http://www.interfax.ru/print.asp?sec=1448&id=226823.

2. T. Maurer, “CyberNormEmergenceattheUnitedNations,” сентябрь 2011г.. [Электронный ресурс]. Режим доступа: http:// www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf.

3. T. Gjelten, “Seeing The Internet As An ‘Information Weapon’,” 23 сентября 2010г.[Электронный ресурс]. Режим доступа: http://www.npr.org/templates/story/story.php?storyId=130052701.

4. International code of conduct for information security, Annex to the letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/66/359), 2011г.

5. OECD, “OECD Council Recommendation on Principles for Internet Policy Making,” 13 декабря 2011г. [Электронный ресурс]. Режим доступа: http://www.oecd.org/dataoecd/11/58/49258588.pdf.

6. K. Giles, “Information Troops: A Russian Cyber Command?,” in Third International Conference on Cyber Conflict, CCDCOE, 2011г.

7. W. Hague, “Chair’s statement,” 2 ноября 2011 г. [Электронныйресурс]. Режимдоступа: http://www.fco.gov.uk/en/news/latest-news/?view=PressS&id=685663282.

8. И. Щеголев, на Лондонской конференции по кибербезопасности, 2011г..

9. С. Модестов, “Пространство будущей войны” Вестник академии военных наук, № 2, 2003г.

10. NDC, “The Indivisibility of Security: Russia and Euro-Atlantic Security,” NATO Defense College, Rome, 2010г.

11. A. Monaghan, “NATO and Russia: resuscitating the partnership,” May 2011. [Электронный ресурс]. Режим доступа: http:// www.nato.int/docu/review/2011/NATO_Russia/EN/index.htm.

12. H. Clinton, “Remarks by Hillary Rodham Clinton at Conference on Internet Freedom, The Hague, Netherlands,” 8 December 2011. [Электронный ресурс]. Режим доступа: http://www.state.gov/secretary/rm/2011/12/178511.htm.

13. A.-M. Taliharm, “Cyberterrorism: in Theory or in Practice?,” Defence Against Terrorism Review, Vol. 3,No. 2, pp. 59-74, 2010.

14. A. Michael, “Cyber Probing: The Politicisation of Virtual Attack,” Defence Academy of the United Kingdom, Shrivenham, 2010.

15. A. Monaghan, “The Moscow metro bombings and terrorism in Russia,” June 2010. [Электронный ресурс]. Режим доступа: http://www.ndc.nato.int/research/series.php?icode=1.

16. Council of Europe, “Convention on Cybercrime,” 23 November 2001. [Электронныйресурс]. Режимдоступа: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

17. V. P. Sherstyuk, Presentation, Brussels, 2011г.

18. Т. Борисов, “Виртуальный мир закрыт”,Российская газета, 12.11.2010 г.

19. Challenges in Cybersecurity - Risks, Strategies, and Confidence-Building, Berlin, 2011.

20. Российское Министерство Обороны, 22 декабря 2011 г. [Электронный ресурс]. Режим доступа: http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle.

21. US Department of Defense, "Strategy for Operating in Cyberspace," July 2011. [Электронный ресурс]. Режим доступа: http:// www.defense.gov/news/d20110714cyber.pdf.

22. В. М. Лисовой, «О законах развития вооруженной борьбы и некоторых тенденциях в области обороны», Военная мысль, № 5, 1993 г.

23. В.И. Цымбал «О концепции информационной войны» // Информационный сборник "Безопасность", № 9, 1995 г.

24. Collective Security Treaty Organisation, "CSTO website," 2012. [Электронный ресурс]. Режим доступа: http://www.odkb.gov.ru/start/index_aengl.htm.

25. Shanghai Cooperation Organisation, 2009. [Электронныйресурс]. Режим доступа: http://www.sectsco.org/EN/show.asp?id=182.

26. ИТАР-ТАСС, 29 января 2009 г.

27. Security Council of the Russian Federation, "Information Security Doctrine of the Russian Federation," 2000г. [Электронныйресурс]. Режим доступа: http://www.scrf.gov.ru/documents/6/5.html.

28. Интерфакс, 12 октября 2000 г.

29. Город Новостей «Я не обижаюсь на вас, когда вы поливаете меня поносом»: Путин пообщался с руководителями СМИ. 19 января 2012 г. [Электронный ресурс]. Режим доступа: http://www.city-n.ru/view/296196.html.

30. Deutsche Welle, "Russia holding back online shutdowns for now, expert says," 13 декабря 2011г. [Электронныйресурс]. Режим доступа: http://www.dw.de/dw/article/0,,15599135,00.html.

31. A. Monaghan, "Flattering to deceive? Change (and continuity) in post election Russia," март 2012г. [Электронныйресурс]. Режим доступа:

http://www.ndc.nato.int/research/series.php?icode=3.

32. Д. Медведев, “Дмитрий Медведев провел во Владикавказезаседание Национального антитеррористического комитета,” 22 февраля 2011 г. [Электронный ресурс]. Режимдоступа: http://www.kremlin.ru/transcripts/10408.

33. Н. Макаров, «Характер вооруженной борьбы будущего» Вестник академии военных наук, 2010г.

34. T. Thomas, Recasting the Red Star, Fort Leavenworth: Foreign Military Studies Office, 2011г.

35. UNIDIR, 2008г. [Электронный ресурс]. Режим доступа: http://www.unidir.org/audio/2008/Information_Security/en.htm.

36. R. Soloveitchik, “Twitter Becomes Key for Moscow Protests,” 23 декабря 2011г. [Электронныйресурс]. Режим доступа: http://www.themoscowtimes.com/arts_n_ideas/article/twitter-becomes-key-for-moscow-protests/450350.html.

37. B. Krebs, “Twitter Bots Drown Out Anti-Kremlin Tweets,” 8 декабря 2011г. [Электронный ресурс]. Режим доступа: http:// krebsonsecurity.com/2011/12/twitter-bots-drown-out-anti-kremlin-tweets/.

38. Forbes, “Дуров: ФСБ просит “ВКонтакте” блокировать оппозиционные группы”, 8 декабря 2011 г. [Электронный ресурс]. Режим доступа: http://www.forbes.ru/news/77291-durov-fsb-prosit-vkontakte-blokirovat-oppozit- sionnye-gruppy.

39. FIIA, Finnish Institute of International Affairs seminar, “Russian Society through the Prism of Current Political Protests”, Helsinki, 2012г.

40. Аргументыи факты, “Николай Патрушев: США прикрываютсясказкамиоправах человека,” 14 декабря 2011г. [Электронный ресурс].

Дата публикации на сайте 25.01.2018