Давыдова-Мартынова Е.И.

ПРОБЛЕМА ЭКСТРЕМИЗМА В ВИРТУАЛЬНОМ ПРОСТРАНСТВЕ СЕТИ ИНТЕРНЕТ*

Данная статья посвящена проблеме информационной безопасности. Особое внимание уделяется использованию ресурсов сети Интернет экстремистами разного толка (неонацистами, расистами, шовинистами и др.) в качестве инструмента пропаганды своих взглядов и мобилизации единомышленников. Автором предлагается комплексный трехуровневый подход к решению обозначенных проблем: международное сотрудничество, разработка эффективных норм национального законодательства, создание технологической системы «контентной фильтрации».

Ключевые слова: *Интернет, информационная безопасность, законодательство, экстремизм, ксенофобия, международное сотрудничество.*

Сегодня сеть Интернет, как средство массовой коммуникации, действительно достигла такого уровня развития и воздействия на общественную жизнь, который требует реального государственного вмешательства в виде реализации уже принятых законов и разработки новых механизмов правового регулирования.

В Доктрине информационной безопасности Российской Федерации подчеркивается, что информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации [1, 4].

Одна из острых проблем информационной безопасности – мобилизация экстремизма в сети общего пользования. Становление и развитие сети Интернет, к которой оказываются неприменимыми все ранее существовавшие механизмы и принципы контроля за информационной средой, обогатило экстремистов разного толка (неонацистов, расистов, скинхедов, шовинистов, религиозных фанатиков) чрезвычайно мощным инструментом пропаганды своих взглядов и мобилизации единомышленников. Сайты, распространяющие идеологию ксенофобии, фашизма, антисемитизма, превосходства белой расы, воинствующего исламизма и т.п., концентрируются сегодня практически во всех странах. Российский сегмент сети Интернет все чаще используется различными террористическими и экстремистскими организациями в целях пропаганды своих идей. Многие сайты базируются на серверах зарубежных стран, и российские правоохранительные органы регулярно сообщают об этом международным партнерам. МВД просит их принять необходимые меры для их закрытия. За последние месяцы было направлено 65 таких запросов, из них 48 - в США и 17 - в Европу. Однако ни на один запрос положительного ответа в МВД не получили [7, 1].

Как справедливо отмечает ведущий научный сотрудник Института мировой экономики и международных отношений РАН Г.Вайнштейн, Всемирная Паутина стала для членов экстремистских и террористических организаций исключительно удобным средством преодоления географической разобщенос-

ти и эффективным способом конспирации и безопасного для них обмена идеями и планами. Опасность выхода экстремистских сил в киберпространство к тому же многократно усугубляется уникальностью Интернета как новейшего средства массовой коммуникации - уникальностью, определяемой не только технологической, но и моральной, этической, правовой спецификой его функционирования [3, 1].

Очевидно, что наибольшая сложность выработки определенных норм и правил, введение которых позволило бы регулировать функционирование сети Интернет, связана с ее транснациональным характером. Любой заслон, воздвигаемый, в частности, перед экстремистскими силами в сетевом сегменте той или иной страны, остается во многом призрачным, поскольку страновые ячейки виртуального пространства, по сути дела, не отделены друг от друга ничем, кроме языковых барьеров.

Дополнительный протокол к Европейской конвенции о борьбе с киберпреступностью трактует «расистские и ксенофобские материалы» как «любые письменные материалы, любое изображение или любое другое представление идей или теорий, которые пропагандируют, способствуют или подстрекают к ненависти, дискриминации или насилию против любой личности или группы лиц, если в качестве предлога к этому используются факторы, основанные на расе, цвете кожи, национальном или этническом происхождении, а также религии» [2, 2].

Ярким примером воздействия ресурсов сети Интернет экстремистского характера стал случай с Александром Копцевым, который был признан виновным в покушении на убийство и разжигании национальной и религиозной розни. Молодой человек признался, что идеи, побудившие его пойти в Московскую хоральную синагогу с ножом, он почерпнул с сайта “Славянского союза”. Названный ресурс и по сей день успешно функционирует в сети. На страничках сайта-книги и тексты выступлений Адольфа Гитлера, материалы, откровенно пропагандирующие движения скинхедов, а также материалы, оправдывающие Холокост, и многое другое. Все это – в открытом доступе. Сайт зарегистрирован в доменной зоне .cc –это региональная зона для доменов островного государства “Кокосовые Острова” (COCOS ISLANDS). Однако управление зоной CC было продано американской компании eNIC Corporation, а регистрация доменов в этой зоне была поставлена на коммерческие рельсы. Сейчас регистрировать домены .cc могут граждане и организации любой страны без ограничений. Этот факт еще раз доказывает, что регулирование ресурсов сети Интернет в отношении защиты информационной безопасности должно быть только международным.

С первой попытки даже начинающий пользователь может получить доступ к информационным ресурсам сайта «Кавказ-Центр», который открыто подстрекает к насилию, разжигает межнациональную и межрелигиозную рознь. Хотя сайт неоднократно «закрывали», он функционирует в Сети и в настоящее время. Так, в 2006 году в Швеции прекратили деятельность Интернет-сайта “Кавказ-Центр”. Закрытие сайта было вызвано тем, что шведская сторона приняла во внимание настоятельные требования российских властей о закрытии этого ресурса. “Кавказ-центр” вел вещание с территории Швеции с 2004 г. Ранее деятельность “Кавказ-центра” аналогичным образом прекращалась на территории Литвы и Финляндии. В настоящее время сайт располагается в коммерческой доменной зоне - .com.

В свободном доступе находятся информационные ресурсы «Партии Свободы». Даже беглый просмотр содержания сайта с уверенностью позволяет заключить, что содержащиеся там материалы имеют расистский и ксенофобский характер. Более того, на страничках сайта - открытые призывы к насилию, а также инструкции для изготовления разного рода экстремистских средств. Следует отметить, что указанный сайт располагается в коммерческой доменной зоне.

Другой пример. Решением Московского городского суда от 19 апреля 2007 года межрегиональная общественная организация "Национал-большевистская партия" была признана экстремистский, а ее деятельность запрещена. Несмотря на вынесенное судебное решение, сайт НБП функционирует в российском сегменте сети Интернет и в доменной зоне .com. Технологический ход, который предприняли разработчики сайта, состоит в том, что на вебстраницах НБП нет материалов с откровенной пропагандой насилия. Но сайт изобилует ссылками на ресурсы, которые размещены в тех зонах сети, которые сложнее контролировать, например, community.livejournal.com (Живой Журнал). На «территории» указанного ресурса обосновались многие идеологи экстремизма в совершенно разных его ипостасях: начиная от национал-большевизма, кончая все тем же сатанизмом. К примеру, есть свой Живой Журнал у известного идеолога сатанизма Варракса. И в нем, и на своем сайте Black Fire Pandemonium он уже не строит "светлое" сатанинское будущее, а борется с инородцами.

Ресурсами сети Интернет для осуществления террористической деятельности воспользовались организаторы взрыва на Черкизовском рынке. В марте 2007 года Замосковорецкий суд Москвы выдал санкции на арест двоих студентов Московского педагогического государственного университета, Николая Качалова и Дмитрия Федосеенкова, обвиняемых по эпизодам преступлений в рамках дела о взрыве на Черкизовском рынке столицы в августе 2006 года. Обвиняемые, по данным Моспрокуратуры, являлись сторонниками РОНСа. В результате взрыва безоболочного устройства погибли 12 человек, в том числе двое детей, а 55 посетителей и работников рынка получили травмы. Следствие установило, что, помимо взрыва на рынке, участники националистической группы совершили еще семь преступлений с использованием взрывчатки, которую изготавливали по рецептам, найденным в сети Интернет.

Перечисленные примеры – лишь малая толика того, чем могут столкнуться пользователи сети Интернет.

Итак, отсутствие единообразного применения законодательства по вопросам представляемой в глобальных сетях информации, а также отсутствие достаточно разработанных технологий фильтрации позволяет размещать в Интернете противоправные материалы откровенно националистического, фашистского, расистского содержания, рецепты производства наркотических и взрывчатых веществ и т.д.

Считаем, что информационная безопасность сетей связи должна обеспечиваться в условиях комплексного подхода, который подразумевает необходимость создания совместимой сетевой инфраструктуры обеспечения информационной безопасности, поскольку уязвимость любого участка сети может создать проблемы для всех её участников. Другими словами, комплексный подход к решению рассматриваемой проблемы должен включать разработку мер по следующим направлениям:

- международно-правовое регулирование;

- разработка эффективного механизма правового регулирования в рамках внутригосударственного права;

- технологическое направление (разработка «контентной фильтрации»).

Большое значение в контексте рассматриваемой проблемы имеет Дополнительный протокол к европейской Конвенции по борьбе с киберпреступностью, принятый 7 ноября 2002 года. Документ обязывает страны ЕС приравнять к уголовным преступлениям любые проявления расизма и ксенофобии в сети: пропаганду идей превосходства одной расы или нации над другими, призывы к дискриминации отдельных групп людей на основании их цвета кожи или принадлежности к определенной религиозной конфессии и т. д. [2, 2].

В протоколе подчеркивается важность борьбы с web-ресурсами и web-серверами, "отрицающими, умаляющими, одобряющими или оправдывающими геноцид или преступления против человечества, в частности, совершенные в период 1941-45 годов". Преступлением признается не только производство и распространение расистских материалов в Интернете, но и размещение гиперссылок на такие материалы на сайтах любой тематики. Кроме того, сервис-провайдерам запрещено предоставлять хостинг (компьютерные "площади") сайтам оговоренной направленности.

В Российской Федерации в основном сформирована нормативная правовая база в сфере противодействия экстремизму и ксенофобии. Вместе с тем, действующее законодательство пока не позволяет достаточно эффективно противодействовать экстремистским и ксенофобским проявлениям во всём их многообразии.

В 2008 году Генеральной прокуратурой Российской Федерации был подготовлен законопроект, предусматривающий перекрытие доступа к Интернет-страницам и закрытие сайтов, публикующих материалы экстремистского характера. В частности, законопроект предлагает устанавливать ответственность за распространение экстремистских материалов в сети Интернет. Так, в соответствии со ст. 13 указанного законопроекта, материалы, размещаемые на сайтах в сети Интернет, признаются экстремистскими федеральным судом по месту их обнаружения или нахождения физического лица либо организации, их разместившей, на основании заявления прокурора или при производстве по соответствующему делу об административном правонарушении, гражданскому или уголовному делу. Одновременно судом принимается решение о прекращении доступа к данным материалам на сайте в сети Интернет. Федеральный список экстремистских материалов и сайтов сети Интернет подлежит размещению в сети Интернет на сайте федерального органа исполнительной власти в сфере юстиции, а также опубликованию в средствах массовой информации.

Пока названный законопроект находится на проработке в Комитете Государственной думы РФ по безопасности, то есть официально на рассмотрение Госдумы он пока не внесен. Предложенные в отношении безопасности в сети Интернет меры могут появиться в уже действующем законе "О противодействии экстремистской деятельности". Разработчики законопроекта считают целесообразным добавить в текст закона новую статью "Ответственность за распространение экстремистских материалов в сети Интернет".

Кроме того, в интересах обеспечения информационной безопасности провайдеры должны принимать меры по выявлению неправомерных действий

потребителей и оказывать помощь силовым структурам в проведении оперативно-розыскных мероприятий. В то же время действия провайдеров связи не должны нарушать прав потребителей на неприкосновенность частной жизни, личную и семейную тайны, тайну переписки, переговоров, свободный доступ к информации и т.д.

Немаловажное значение имеет и разработка новейших технологий в сфере информационной безопасности. Например, специалистами разрабатывается так называемая "контентная фильтрация" - технология, обеспечивающая отсеивание негативной информации (порнографии), вирусов и спама. Речь идет о создании программного средства, с помощью которого российские пользователи на индивидуальном уровне или администраторы локальных сетей могли бы блокировать доступ с подконтрольных им компьютеров к сайтам, на которых содержится информация, вступающая в конфликт с действующим законодательством или противоречащая нормам общественной морали.

В заключение хотелось бы еще раз подчеркнуть, что в нахождении баланса интересов важную роль играет разработка комплексного подхода, включающего:

- расширение международного сотрудничества в области исследования и анализа законодательств и нормативных баз различных стран, обмена информацией, создания систем оповещения и предупреждения;

- разработку эффективных норм российского законодательства;

- создание действенной технологической системы «контентной фильтрации».

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации // Российская газета. 2000. 28 сентября. С. 4.
2. Дополнительный протокол к Конвенции о преступлениях в сфере компьютерной информации относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем ETS N 189 (Страсбург, 28 января 2003 г.)// Справочно-правовая система «Гарант», 15 сентября 2007 г.
3. Вайнштейн Г. Экстремизм в Интернете: как обуздать?// www.politcom.ru
4. Мелюхин И. О зарубежном опыте регулирования Интернета // ВИНИТИ. – Сер. 1. – 1998. – № 3.
5. Официальный сайт МВД http://www.mvdinform.ru/news/10684. Дата посещения 1 марта 2008 г.

E. DAVIDOVA-MARTINOVA

EXTREMISM PROBLEM IN VIRTUAL SPACE OF THE INTERNET

Moscow state regional university

The article below is devoted to the problem of information safety. The special attention is given to the use of resources of the Internet extremists of different sense (neo-Nazis, racists, chauvinists, etc.) as a mean of propaganda of positions and mobilization of adherents. The author offers a complex three-level approach to the decision of the problem: the international cooperation, development of effective norms of the national legislation, creation of the technological system of a filtration.

Key words: Armed forces of Russia, social problems, food maintenance, health of military men, housing problem, social moods.