(cc) BY

Герасимова Алина Романовна

курсант

Максимов Виталий Алексеевич

канд. юрид. наук, старший преподаватель, майор полиции

ФГКОУ ВПО «Санкт-Петербургский университет МВД России»

г. Санкт-Петербург

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИЗМУ В СЕТИ ИНТЕРНЕТ

Аннотация: *в данной статье рассмотрены проблемы, связанные с информационным экстремизмом в сети Интернет. Процесс глобализации способствовал появлению различных механизмов и средств, используемых экстремистами в своей деятельности. Выделяются такие проблемы, как недостаточное международное регулирование, привлечение в качестве экспертов ученых филологов, технические проблемные аспекты и ряд других. В заключение делается вывод о необходимости комплексного подхода в борьбе с экстремизмом в сети Интернет.*

Ключевые слова: *информационный экстремизм, сеть Интернет, глобализация, международно-правовое регулирование, ответственность, судебная лингвистическая экспертиза, информационно-коммуникационные технологии.*

Современное общество характеризуется наличием сверхскоростных систем передачи сообщений, информации. Всемирная информационная сеть Интернет позволяет индивидам, группам, общностям обмениваться информацией в любое время суток, в любом регионе, что свидетельствует о снятии пространственно-временных границ. Положительной стороной данного явления является возможность интеллектуального развития, самообразования, ведения бизнеса. Однако есть и отрицательные аспекты, таки как, например, использование достижений научно-технического прогресса антисоциальными элементами социума. При этом в настоящее время крайне слабо развито научное прогнозирование угроз и

рисков, связанных со сферой социального управления, в правоохранительной системе. В связи с этим возникает необходимости уделить повышенное внимание особенностям глобального информационного общества, его системообразующим элементам, а также определенным коммуникационным структурам и явлениям, в совокупности детерминирующим рост угроз информационного экстремизма, а также информации, способствующей возникновению феномена готовности к экстремистской деятельности (экс-тремпарантности) [1, с. 309–313].

Процесс глобализации активно используется организаторами и участниками экстремистских групп, которые принимают на вооружение новейшие информационно-коммуникационные технологии, делающих менее уязвимыми для правоохранительных органов элементы их инфраструктуры. Увеличивается потенциал террористических организаций в современных информационных условиях, в основу построения которых заложен принцип сетевой структуры. Для данных организаций характерны единые центры и информационно-коммуникативные каналы, автономный способ существования входящих в сообщество периферийных преступных группировок, взаимодействующих как с центром, так и между собой [2].

Кроме этого, одной из проблем является недостаточное нормативно-правовое регулирование в рамках международного взаимодействия государств в сфере противодействия экстремизму и терроризму в информационно-коммуникационном пространстве. Также различные государства избирают отличные друг от друга подходы к нормативно-правовому регулированию антиэкстремистской деятельности, что не способствует эффективному сотрудничеству в борьбе с экстремизмом в сети Интернет.

Вместе с тем, существуют проблемные вопросы технического плана. Фактически невозможно установить лицо, разместившее в сети экстремистский или террористический материал, этому способствуют современные технологии беспроводного доступа в сеть, имеющиеся в свободной продаже сетевые платы с динамическим IP-адресом и т. п. К тому же, возникают трудности с идентифика-

цией лица в качестве автора или издателя экстремистского или террористического материала, так как типичным примером является идентификация лица, просто как владельца средства вычислительной техники, посредством которого в сети был размещен материал [3, с. 143–147].

Важно также учитывать, что в сети Интернет информация экстремистского содержания может содержаться в различной форме: текстуальной и графической (рисунки, фотографии, видеоизображения и т. д.). Для установления направленности указанной информации на возбуждение ненависти либо вражды, а также на унижение достоинства человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе возникает необходимость использования специальных знаний [4, с. 125–127]. В научной литературе отмечается, что в настоящий момент накоплен значительный опыт применения судебных гуманитарных (лингвистических) экспертиз в ходе расследования криминальных проявлений экстремизма, которые помогают решать вопрос о наличии экстремистских призывов и пропаганды. Анализируя следственную практику, можно сделать вывод о том, что к проведению судебных лингвистических экспертиз часто привлекаются авторитетные ученые филологи, не являющиеся сотрудниками специализирующихся на данной экспертизе государственных учреждений. Основу их выводов составляют непроверенные версии, гипотезы, субъективные мнения, которые могут быть подходящими в сфере научных изысканий, но не приемлемы в качестве выводов экспертизы.

Ещё один немаловажный вопрос, связанный с распространением экстремистских материалов в сети Интернет, это вопрос ответственности модераторов, операторов связи и провайдеров. Во-первых, возникает вопрос, относится ли деятельность провайдеров к «содействию в указанных деяний организации, подготовке и осуществлении, в том числе путем предоставления учебной, полиграфической и материально-технической базы, телефонной и иных видов связи или оказания информационных услуг», как это указано в ст. 1 Федерального закона

«О противодействии экстремистской деятельности» [5]. Во-вторых, важно определиться с критерием вменения им ответственности. Мировая практика свидетельствует о неоднозначности решения данного вопроса, но в большинстве стран преобладает субъективное вменение: провайдер, который предоставляет хостинг знал о содержании информации либо не знал, но по обстоятельствам дела должен был или мог знать об этом [6, с. 306–310]. Другим критерием привлечения к ответственности выступает наличие технических возможностей у провайдеров блокировать передачу незаконной информации. При этом, стоит отметить, что в российской системе уголовного права данный вариант вменения невозможен, так как ответственность юридических лиц отсутствует, в связи с этим нужно искать альтернативные механизмы привлечения к уголовной ответственности.

Таким образом, современные реалии позволяет заметить потребность в жестких мерах по пресечению экстремистских действий в сети Интернет. Информационные экстремисты хорошо оснащены в техническом и технологическом плане, также осознают возможность безнаказанности своих действий в силу сложности установления автора экстремистских материалов. Вследствие этого необходимо комплексный подход, включающий усилия ученых, общественности, силовых структур и администраций всех уровней для решения проблемы противодействия экстремизму в сети интернет.

Список литературы

1. Мозговой В.Э. Информационный экстремизм в условиях глобализации и информатизации социума // Общество и право. – 2015. – №1 (51).

2. Принципы борьбы с экстремизмом в сети и вне ее будут одинаковыми / Официальный сайт информационного портала SecurityLab.ru [Электронный ресурс]. – Режим доступа: http:// www.securitylab.ru/news.html (дата обращения: 25.05.2016).

3. Троегубов Ю.Н. Проблемы противодействия экстремизму в сети интернет // Гуманитарный вектор. Серия: История, политология. – 2014. – №3 (39).

4. Валеев А.Х. Борьба с проявлением экстремизма в сети интернет // Бизнес в законе. Экономико-юридический журнал. – 2011. – №6.

5. Федеральный закон от 25.07.2002 №114-ФЗ (ред. от 23.11.2015) «О противодействии экстремистской деятельности» // «Собрание законодательства РФ». – 29.07.2002. – №30. – Ст. 3031.

6. Лунева Е.Н. Проблемы привлечения к уголовной ответственности при осуществлении экстремистской деятельности в сети интернет // Science Time. – 2015. – №1 (13).

7. Максимов В.А. Институт публичного обещания награды в деятельности правоохранительных органов // Современная наука. – 2014. – №2. – С. 11–15.

8. Максимов В.А. Роль и место министерства внутренних дел России в правоотношениях из публичного обещания награды за предоставление сведений, имеющих значение для правоохранительных органов // Современная наука. 2014. – №1. – С. 8–9.