Секция «Информационное обеспечение внешней политики»

# Анализ технологий интернет-пропаганды, используемых террористическими организациями, и стратегий борьбы с ними

**Научный руководитель – Грачев Сергей Иванович**

***Богачев Александр Дмитриевич***
*Студент (магистр)*
Нижегородский государственный университет им. Н.И. Лобачевского, Нижний Новгород, Россия
*E-mail: bogachev.95@list.ru*

Террористические организации все чаще используют новые интернет-технологии для расширения своего влияния и массового распространения экстремистской пропаганды. По мнению специалистов, развитие интернет-технологий привело к росту пропаганды и привлечения новых членов, чему способствовали существующие проблемы исламских сообществ. Легкодоступность и анонимность, предоставляемые онлайн-пространством, позволили террористическим группам легче и без угрозы раскрытия, использовать в своих целях интернет-ресурсы.

В конце 1990-х годов террористические организации начали использовать интернет-технологии для продвижения своих идей и получения денег. К 1999 году Интернет стал главной ареной для распространения экстремистской пропаганды [1]. В настоящее время члены террористических организаций по всему миру получают всю необходимую информацию через различные онлайн каналы. К 2005 году 40 террористических организаций содержали более 4500 веб-сайтов. Развитие YouTube позволило широко распространять профессионально выглядящую аудиовизуальную пропаганду.

В 2000-х годах, с появлением социальных сетей, появилась новая среда для распространения террористической пропаганды. В отличие от технологий 1990-х годов, социальные сети позволили расширить географию вербовки и иметь обратную связь с потенциальными террористами и своими ячейками. [1]

С точки зрения, террористических организаций, использование интернет-площадок для распространения пропагандистских сообщений и привлечения новых членов достаточно эффективно. Новые медиа-технологии не требуют наличия большого числа ресурсов и специализированных навыков, кроме того, высокие уровни анонимности позволяют снизить риск раскрытия властями. [2]

Учитывая рост популярности, которую современные террористические организации приобрели благодаря использованию интернет-технологий, становится ясно, что необходимы серьезные меры для того, чтобы остановить распространение экстремистских материалов в Интернете. Необходимо признать, что действия по борьбе с террористической пропагандой в интернете могут привести к ограничению некоторых гражданских свобод, которые сейчас считаются незыблемыми, в обмен на большую безопасность и защиту от терроризма.

Правительства во всем мире заимствовали комбинацию из трех общих стратегий, которые касаются интернет-пропаганды экстремизма:

1. Стратегия жестких действий, которая направлена на подавление онлайн-экстремистской деятельности
2. Стратегия мягкой силы, направленная на борьбу с радикализацией путем использования контраргументов и продвижения плюрализма мнений;

3. Стратегия, основанная на разведке, которая использует онлайн-экстремистскую деятельность и информацию, которую она предоставляет для выявления и физического преследования лиц, вовлеченных в терроризм. [3]

Большинство правительств демонстрируют некоторые элементы политики «отказа в доступе и / или удаления экстремистской информации» в подходе к работе с интернет-ресурсами, которые занимаются террористической пропагандой или привлечением новых членов. Однако в большинстве случаев применения данной стратегии, технологические инновации и невнимание к деталям со стороны тех, кто выполняет блокировку / удаление, не позволили использовать этот метод борьбы с радикализацией.

Технологические достижения и динамический характер Интернета не позволяют эффективно осуществлять контроль за контентом. Так же быстро, как обрабатывается один сайт / группа / приложение, возникает альтернатива заблокированному контенту.

Альтернативная стратегия предполагает использование мягкой силы и дипломатических методов для противодействия распространению экстремистской информации. В целях ее реализации привлекаются как правительственные органы, так и региональные умеренные исламские общественные группы для распространения антиэкстремистских материалов, которые бросают вызов той риторике, которая используется онлайн-террористами [1].

Последняя из трех представленных стратегий включает использование разведывательных служб для сбора информации о террористических группах и планирования операций против них. Эта стратегия включает в себя преимущественно скрытый сбор информации и не стремится напрямую вмешиваться в пропагандистский контент, который публикуется в Интернете.

### Источники и литература

1) Dean, G., Bell, P. and Newman, J., 'The Dark Side of Social Media: Review of Online Terrorism', Pakistan Journal of Criminology, vol. 4, no. 2, 2012, http://go.galegroup.com/ps/i.do?id=GALE%7CA313840278&v=2.1&u=macquarie&it=r&p=EAIM&sw=w&asid=0c5d2400e5ffe21de5ed44f219358017

2) Agarwal, S., Applying Social Media Intelligence for Predicting and Identifying On-line Radicalization and Civil Unrest Oriented Threats, https://arxiv.org/pdf/1511.06858.pdf

3) C. Leuprecht and D. Skillicorn, 'Radicalisation: What (If Anything) is to be Done? When Facts Get in the Way of a Good Story', Home Team Journal, №3, 2011, стр. 38-46, https://www.mha.gov.sg/HTA/Documents/Home%20Team%20Journal%20Special%20Edition%20-%203rd%20issue.pdf