

ОБЗОР ИССЛЕДОВАНИЙ НА ТЕМУ ПРОТИВОДЕЙСТВИЕ ТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В СЕТИ ИНТЕРНЕТ

*Д. А. Виноградова, аспирант, гр. А0-39
Томский политехнический университет
E-mail: dak38@tpu.ru*

Введение

Терроризм – это опаснейшая глобальная проблема современности, создающая серьезную угрозу безопасности всего общества.

Ряды террористов пополняются путем радикализации общества. Радикализация представляет из себя процесс постепенного принятия террористических идей и плавного перехода от умеренных и нейтральных взглядов на политическую или социальную ситуацию в обществе к экстремальным и радикальным. В наши дни, Интернет играет ключевую роль в процессе радикализации. Для террористов Интернет является главным средством для распространения экстремистских идей в массы и для вербовки новичков. Радикализация происходит в несколько этапов. На начальном этапе радикализации многие люди могут просто испытывать некоторую неудовлетворенность окружающим миром, которую время от времени выражают в своих постах и комментариях, как пользователи социальной сети. Чтобы как-то заглушить эту неудовлетворенность, люди начинают интересоваться любой информацией в Интернете, которая поможет уменьшить это неприятное чувство. На данном этапе многие сталкиваются с информацией террористического характера, многих она может заинтересовать, хотя бы просто для ознакомления. В процессе изучения террористической информации, рано или поздно, некоторая часть людей произведет контакт с террористами-вербовщиками, которые, часто, хорошо знают свое дело и с легкостью переманивают в свои ряды морально ослабленных людей. Или же наткнутся на закрытое террористическое онлайн-общество, которое является своеобразной эхо-камерой, где террористические идеи и убеждения усиливаются до крайней степени, что порождает террористов-одиночек. Таким образом, сдерживание процесса радикализации в Интернете стало важным и необходимым процессом в вопросе обеспечения государственной безопасности любой страны.

Помимо пополнения своих рядов, сеть Интернет пользуется высокой популярностью среди террористов, как средство связи между собой, потому что именно в Интернете можно вести любой диалог, оставаясь при этом в полной анонимности, тем самым избегая прямого контакта между собой, что сокращает риск быть пойманным по вине другого менее осторожно террориста.

В данной работе проведен обзор технических исследований на тему ограничения распространения радикальной деятельности в сети с целью выявления основных направлений технических методов борьбы с терроризмом в Интернете.

Обзор исследований противодействия террористической деятельности в сети Интернет

В процессе ознакомления с технической литературой были выявлены следующие направления исследований по противостоянию террористической деятельности в сети.

Классификация радикализирующего интернет-контента

Первое направление исследований – это классификация интернет-контента, как радикализирующего. Данная стратегия борьбы с процессом радикализации направлена на поиск в сети террористической информации для ее дальнейшего блокирования. Данная стратегия рассматривается во многих литературных источниках.

В общем виде методы классификации радикализирующего контента имеют следующие этапы:

1. Поиск контента для анализа. Используются технологии отслеживания ссылок, которые берут контент для анализа со страниц, ссылки на которые находились среди контента страницы, содержащей террористическую информацию.
2. Анализ контента. Используются технологии классификации текста на основе словаря или машинного обучения, чтобы определить является ли контент радикализирующим.

Идентификация террористических аккаунтов

Еще одно направление исследований – это поиск в сети аккаунтов, принадлежащих террористам или же людям, которые еще не являются террористами, но уже находятся на пути радикализации.

Надо отметить, что поиск террористов в сети является сложной задачей. Обычно, террористы, то есть люди, кто уже принял радикальные идеи и принимает участие в террористической деятельности, ведут в сети двойную жизнь и имеют строгий, проверенный протокол поведения в сети, который обеспечивает им полную скрытность. Однако, в [1] утверждается, что в жизни террористов существуют фазы их деятельности, когда конфиденциальность информации о их радикальной жизни ослаблена больше всего, когда террористы теряют бдительность и начинают нарушать свой протокол. Перечислим эти фазы:

1. Фаза радикализации и начала террористической жизни. Это период, когда человек только вливается в ряды террористов и еще не знает, как именно нужно себя вести в сети.
2. Фаза организации террористического акта.
3. Фаза, когда человек хочет закончить свою радикальную деятельность и покинуть свою террористическую организацию.

Каждая из перечисленных фаз происходит в тот период жизни террориста, когда его переполняют эмоции, когда можно наблюдать скачки настроения. Поэтому данное направление исследований всегда построено на технологиях анализа настроения, эмоций или тональности контента [1-3].

Построение и анализ социальных графов

Последнее направление исследований по контролю террористической деятельности в сети заключается в построение и анализа социальных графов.

Социальный граф в данных исследования представляет собой взвешенный ориентированный граф, построенный на основе данных, выбранных из социальных сетей на определенную тематику, каждая вершина которого представляет собой один из аккаунтов социальной сети, а ребра представляют вектор признаков связи двух соединенных аккаунтов. По сути, социальный граф отображает взаимодействия одного террористического онлайн-сообщества.

Цели исследований данного направления обычно сводят к определению ролей в структуре сообщества каждого представителя: поиск структуры террористического сообщества, идентификация главных фигур сообщества и т.п. Для достижения целей в процессе анализа социальных графов применяют такие действия, как кластеризация графа, идентификация ключевых узлов графа, выявление подграфов.

Часто исследования данного направления сочетают в себе методы анализа социальных графов с другими технологиями: интеллектуальный анализ контента, анализ текста, анализ настроений и анализ мнений. Например, Вадхва и др. объединили методы анализа текста и анализа социальных сетей для прогнозирования динамики поведения экстремистских сообществ [4].

Заключение

В данной статье был проведен анализ технической литературы на тему противостояния кибертерроризму и процессу радикализации в сети. Были выявлены основные направления исследований: классификация радикализирующего интернет-контента, идентификация террористических аккаунтов, построение и анализ социальных графов. Выявлены основные технологии и методы: анализ текста на основе словаря, анализ текста на основе методов машинного обучения, анализ настроения, анализ тональности и т.д.

Список использованных источников

1. The spider-man behavior protocol: exploring both public and dark social networks for fake identity detection in terrorism informatics / M. Cristani, E. Burato, K. Santac'a, C. Tomazzoli // Knowledge Discovery on the WEB. - 2015
2. Araque O. An Approach for Radicalization Detection Based on Emotion Signals and Semantic Similarity / O. Araque C.A. Iglesias // IEEE Access. – 2020. – Vol. 8. – P. 17877-17891. – doi: 10.1109/ACCESS.2020.2967219
3. Pelzer R. Policing of Terrorism Using Data from Social Media // European Journal for Security Research. - 2018. - Vol. 3. - P. 163-179. - doi: 10.1007/s41125-018-0029-9
4. Wadhwa P, Bhatia M P S. An Approach for Dynamic Identification of Online Radicalization in Social Networks // Cybernetics and Systems. – 2015. – Vol. 46, Iss. 8. – P. 641-665. – doi: 10.1080/01969722.2015.1058665