



**ПРОКУРОРСКАЯ ДЕЯТЕЛЬНОСТЬ; СУДЕБНО-ЭКСПЕРТНАЯ ДЕЯТЕЛЬНОСТЬ;
ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ**

УДК 340

Хованов Илья Сергеевич

Орловский государственный университет имени И. С. Тургенева

Россия, Орел

khovanov.i@yandex.ru

Khovanov Ilya

Oryol State University named after I.S. Turgenev

Russia, Orel

**О НЕКОТОРЫХ ПРОБЛЕМАХ ПРОТИВОДЕЙСТВИЯ ПРОКУРАТУРОЙ
РОССИЙСКОЙ ФЕДЕРАЦИИ ЭКСТРЕМИЗМУ В ИНТЕРНЕТЕ**

Аннотация: в статье рассмотрены некоторые проблемы противодействия прокуратурой РФ экстремизму в интернете. Актуальность работы обусловлена ростом преступлений экстремистской направленности в последние годы. В качестве основной проблемы выделяется необходимость повышения эффективности мониторинга интернета на предмет выявления экстремистского контента. Предлагается централизовать интернет-мониторинг в рамках подразделения по надзору за кибербезопасностью Генпрокуратуры РФ и создать специализированное программное обеспечение для автоматизированного поиска экстремистского контента. Представляется, данные нововведения повысят эффективность противодействия распространению экстремизма в интернете.

Ключевые слова: экстремизм, интернет, мониторинг, контент, прокуратура, информационное пространство, программное обеспечение

**ON SOME PROBLEMS OF COUNTERACTION OF EXTREMISM IN THE
INTERNET BY THE PROSECUTOR'S OFFICE OF THE RUSSIAN
FEDERATION**



Annotation: the article considers some problems of counteraction of extremism on the Internet by the RF prosecutor's office. The relevance of the work is due to the growth of extremist crimes in recent years. As the main problem the necessity of increasing the efficiency of Internet monitoring for detection of extremist content is emphasized. It is proposed to centralize Internet monitoring within the cybersecurity oversight unit of the Prosecutor General's Office of the Russian Federation and to create specialized software for automated search of extremist content. According to the author, this will improve the effectiveness of countering the spread of extremism on the Internet.

Key words: extremism, Internet, monitoring, content, prosecutor's office, information space, software

В последние годы в России отмечается рост преступлений экстремистской направленности. Согласно информации с сайта Генеральной прокуратуры РФ, если в 2019 году было зарегистрировано 585 преступлений экстремистской направленности, то в 2022 году - уже 1566 [10], следовательно, за 3 года количество зарегистрированных преступлений выросло на 267,69%. Президент Российской Федерации В.В. Путин заявил, что «Экстремизм — прямая угроза единству России, необходимо жестко пресекать любые его проявления.» [13]. В связи с этим была принята «Стратегия противодействия экстремизму в Российской Федерации до 2025 года» [1].

Одним из способов распространения материалов, содержащих в себе признаки экстремистской направленности, является интернет, который дает людям возможность анонимно выражать любые взгляды, в том числе экстремистские, что снижает ответственность и раскрепощает. В сети легко найти единомышленников и создавать закрытые сообщества, где радикальные взгляды усиливаются. Это создает эффект "эхо-камеры", что может приводить к радикализации.



Кроме того, в современных реалиях немаловажной проблемой становится распространение дезинформации, которая появляется в сети и может применяться виновными лицами для набора сторонников.

Люди подвержены манипуляциям. В целом, распространение экстремистских идей в интернете может затрагивать различные группы людей. Однако наиболее уязвимы к этому молодежь и люди, испытывающие социальную изоляцию или недовольство своим положением. Зачастую молодые люди, которые находятся в поиске идентичности или испытывают проблемы с социализацией, могут быть восприимчивы к радикальным идеям. Интернет дает им возможность найти сообщества единомышленников и чувство принадлежности. Люди, чувствующие себя отверженными обществом, маргинализированные или ущемленные в правах группы также могут быть более подвержены экстремистской пропаганде. Однако, экстремизм может привлекать разных людей, испытывающих недовольство своей жизнью.

Некоторые площадки и сайты с целью увеличения трафика и дохода специально привлекают людей, которые разделяют или готовы проникнуться идеями экстремистов. Многие из данных способов привлечения являются скрытыми, и пользователь не сразу понимает, куда он попал, и какие цели преследует автор данного контента. К ним относятся:

а) создание привлекательного имиджа - экстремистские группы часто позиционируют себя как "защитников угнетенных", борцов за справедливость, обещают чувство общности и значимости для тех, кто присоединится;

б) обещание радикальных решений острых социальных проблем - экстремисты обещают быстро и силовым путем решить проблемы, с которыми борется общество, в том числе социальное неравенство, коррупцию;

в) распространение теорий заговора - утверждения, что власти/элиты/меньшинства якобы угнетают и контролируют народ, манипулируют им.



г) использование интернет-мемов и юмора - мемы, шутки, ирония помогают привлечь молодежь и сделать экстремистские идеи более "трендовыми";

д) целенаправленная вербовка - в закрытых онлайн-сообществах происходит активный поиск и обработка людей, уязвимых для вовлечения в радикальную деятельность; вовлечение через онлайн-игры - использование многопользовательских игр и игровых платформ для распространения экстремистского контента и вербовки.

Указанные выше способы не являются единственным, однако правоприменительная практика свидетельствует о том, что именно они порождают недоверие и подталкивает к радикальным действиям;

В этой связи остро встает вопрос о необходимости повышения качества и эффективности мониторинга интернета на предмет выявления экстремистского контента. Аналогичной позиции придерживается А.И. Бастрыкин, по мнению которого современные технологические достижения и развитие информационных технологий создают новые возможности для совершения преступлений, особенно в сфере киберпреступности. В этой связи автор предлагает принять дополнительные меры по защите информационного пространства. Кроме того, он также указывает на необходимость усилить работу по в сети Интернет материалов экстремистского характера. Увеличение мониторинга интернета и противодействия распространению опасной информации, по мнению главы СК РФ, необходимо для обеспечения безопасности граждан и защиты информационного пространства [14].

Правоприменительная практика правоохранительных органов свидетельствует, что существующий опыт борьбы с экстремизмом в России показывает, что в связи с ростом интернета, а также количества пользователей традиционные методы становятся неэффективными.



Кроме того, на немаловажное значение на надзорную функцию органов прокуратуры в рамках противодействия экстремизма оказывают такие проблемы, как:

1. Перегруженность сотрудников прокуратуры, которые занимаются осуществлением надзора за противодействием экстремизму-объемом противоправной информации в интернете, отсутствует возможность оперативного реагирования; В рамках рассматриваемой самой системы прокуратуры мониторинг осуществляется на уровне всех подразделений структуры, что так же выглядит нецелесообразным.

2. Приказ Генерального прокурора Российской Федерации от 21 марта 2018 г. N 156 [3], не решает появившиеся проблемы, так как не предусматривает мониторинг сети Интернет с помощью специализированного программного обеспечения, которое может анализировать больший объем данных, чем человек.

3. В настоящее время мониторинг осуществляется одновременно различными государственными органами – Прокуратурой РФ, МВД РФ, ФСБ РФ, СК РФ, Министерство Юстиции РФ, Роскомнадзором, НЦпТИ, РОЦИТ, ЦИСМ и иными, что приводит к дублированию полномочий и неэффективному расходованию, как органов прокуратуры, так и государственных структур.

В связи с этим, представляется целесообразным централизовать систему мониторинга интернет-пространства на предмет выявления экстремистского контента в рамках, созданного в формате реализации нацпроекта "Цифровая экономика" [2] подразделения по надзору за кибербезопасностью Генеральной прокуратуры Российской Федерации, создать специальное программное обеспечение, осуществляющее автоматизированный мониторинг интернета на предмет выявления признаков экстремистской деятельности.

Схожую мысль, хоть и в ином контексте описывает А.А. Кульпин, указывая на необходимость цифровой трансформации органов прокуратуры РФ.



По мнению автора, в соответствии с приказом ГП РФ от 14.09.2017 г. № 627 [4] потребность в цифровизации деятельности органов прокуратуры РФ по-прежнему остается актуальной [5, с. 169].

При этом, как справедливо отметили Б.В. Андреев и О.А. Инсаров, в органах прокуратуры отсутствуют единые стандарты разработки и эксплуатации информационных систем, а также на недостаточном уровне находится автоматизация контрольно-надзорной деятельности [6, с. 36]. Полагаем необходимым отметить, что обозначенная проблема не нова. Ранее она была объектом научного исследования таких ученых, как Б.В. Андреев, О.А. Инсаров, А.А. Кульпин и др.

В этой связи, представляется обоснованным также обратиться к зарубежному опыту.

Так, например, в США используют веб-паука The Dark Crawler для сбора и анализа экстремистского контента в интернете [7, с. 179]. Данный инструмент может осуществлять рекурсивный поиск и сбор контента по заданным ключевым словам и параметрам. TDC может автоматически обходить ссылки на сайтах и собирать соответствующий контент, проводить сбор данных с ограничением по количеству веб-страниц, доменов, исключаемых доменов и наличию ключевых слов, что позволяет настроить выборку данных под конкретные задачи. Одной из функций является анализ собранного контента на наличие экстремистских материалов на основе классификации текстов и изображений. TDC может определять уровень радикальности контента, а также выявление скрытых сообществ и групп пользователей по интересам на основе анализа связей между веб-ресурсами. Данное программное обеспечение помогает обнаруживать экстремистские группы, может строить семантические сети на основе собранных данных, что позволяет выявлять ключевые темы, узлы и связи внутри радикальных сообществ.



Интересным является опыт Великобритании в сфере противодействия экстремизму в сети. Система разработана британской компанией ASI Data Science совместно с Министерством внутренних дел Великобритании. Она использует методы машинного обучения для анализа аудио и видеоконтента на предмет выявления признаков экстремистских материалов. Согласно заявлениям создателей, точность распознавания составляет до 99,995% [8]. Так из миллиона анализируемых ею случайно выбранных видеороликов только в пятидесяти случаях потребуется дополнительная экспертиза со стороны человека.

По задумке разработчиков, система должна интегрироваться в инфраструктуру онлайн-платформ для выявления нежелательного контента до его публикации, что позволит значительно сократить распространение, в частности, террористической пропаганды.

При этом, полагаем необходимым отметить, что в настоящее время прокуратуры РФ начинают пробовать использовать аналогичные системы отечественного производства в тестовом режиме. Так, например, в 2015 г. прокуратурой Татарстана был разработан информационно-аналитический комплекс для автоматизированного поиска запрещенного контента в интернете. С июля по декабрь 2015 года с помощью этой системы выявлено более 17 тысяч интернет-страниц с возможными признаками распространения запрещенной информации о наркотиках, экстремизме, суициде, детской порнографии и азартных играх, часть из них заблокирована.

Автоматизированные системы модерации контента могут быть эффективным инструментом борьбы с распространением незаконных материалов в интернете. Однако их применение требует тщательного контроля, чтобы избежать нарушения прав пользователей и превращения в инструмент цензуры. Необходимы дополнительные исследования для оценки реальной эффективности и безопасности подобных технологий.



По нашему мнению, внедрение и создание такого рода отечественных систем, которые в онлайн режиме будут отслеживать весь интернет-трафик на содержание экстремизма, значительно облегчит работу сотрудников прокуратуры и правоохранительных органов.

Международное сотрудничество имеет важное значение в сфере противодействия экстремизму и терроризму, что подтверждается рядом примеров взаимодействия России с другими странами.

Так, Россия активно сотрудничает в рамках Шанхайской организации сотрудничества (ШОС) по вопросам борьбы с экстремизмом. В частности, в сентябре 2018 года в Душанбе прошло очередное шестнадцатое совещание генеральных прокуратур стран-членов ШОС, посвященное противодействию международному терроризму и экстремизму. Участники обсудили меры по усилению борьбы с экстремизмом, противодействию использованию интернета в экстремистских целях, расследованию преступлений экстремистского характера. Был подписан протокол о намерении усилить совместные усилия в этом направлении [9].

Кроме того, Россия развивает двусторонние отношения с ОАЭ в сфере противодействия экстремизму. В декабре 2018 года прокуратуры двух стран заключили меморандум о взаимопонимании, предусматривающий сотрудничество по борьбе с терроризмом и экстремизмом. Генпрокурор России Игорь Краснов в ходе визита в ОАЭ отметил важность объединения усилий в борьбе с киберпреступностью, использованием криптовалюты в преступных целях, финансированием терроризма. Такой обмен опытом между правоохранительными органами двух стран позволит выработать эффективные меры противодействия современным вызовам [11].

Активно развивает Россия сотрудничество в сфере борьбы с экстремизмом и с Беларусью. В октябре 2022 года генеральные прокуроры двух стран договорились о взаимодействии для пресечения экстремистской деятельности, в



том числе в интернете. Была отмечена важность обмена информацией и координации усилий для более результативного противодействия угрозам экстремизма и терроризма [12].

Примеры сотрудничества России на международной арене демонстрируют, что объединение усилий в борьбе с экстремизмом является ключевым для эффективного противодействия этой угрозе.

Таким образом, подводя итоги проведенного исследования, полагаем обоснованной инициативу централизации интернет-мониторинга в рамках подразделения по надзору за кибербезопасностью Генеральной прокуратуры РФ, а также создания и использования данным ведомством специализированного ПО в целях выявления угроз экстремистского характера представляется обоснованной и целесообразной мерой для повышения эффективности противодействия распространению экстремизма в сети Интернет.

Все это позволит снять нагрузку со всех звеньев системы прокуратуры, с органов МВД, ФСБ, СК, осуществляющих мониторинг сети Интернет, сократить время реагирования на угрозы общественной безопасности в информационном пространстве.

Список литературы:

1. Указ Президента РФ от 29 мая 2020 г. № 344 “Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года” / [Электронный ресурс] // Официальные сетевые ресурсы Президента России : [сайт]. — URL: <http://www.kremlin.ru/acts/bank/45555> (дата обращения: 31.07.2023).

2. Постановление Правительства РФ от 2 марта 2019 г. N 234 "О системе управления реализацией национальной программы "Цифровая экономика Российской Федерации" (с изменениями и дополнениями) / [Электронный



ресурс] // Система Гарант : [сайт]. — URL: <https://base.garant.ru/72190034/> (дата обращения: 31.07.2023).

3. Приказ Генерального прокурора Российской Федерации от 21 марта 2018 г. № 156 «Об организации прокурорского надзора за исполнением законов о противодействии экстремисткой деятельности» / [Электронный ресурс] // СПС «КонсультантПлюс»: [сайт]. — URL: https://www.consultant.ru/document/cons_doc_LAW_298172/ (дата обращения: 31.07.2023).

4. Приказ Генерального прокурора Российской Федерации от 14.09.2017 № 627 «Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года» (вместе с «Концепцией цифровой трансформации органов и организаций прокуратуры Российской Федерации до 2025 года») / [Электронный ресурс] // СПС «КонсультантПлюс». : [сайт]. — URL: https://www.consultant.ru/document/cons_doc_LAW_278651/ (дата обращения: 31.07.2023).

5. Кульпин А. А. Конструктор актов прокурорского реагирования, как необходимый элемент цифровой трансформации органов прокуратуры РФ/ А. А. Кульпин // Альманах молодого исследователя. - 2023. - № 14. – С. 169–173.

6. Инсаров О.А., Андреев Б.В Цифровая трансформация органов прокуратуры Российской Федерации // Вестник университета прокуратуры Российской Федерации. 2018. № 5. – С. 36–41.

7. Ryan Scrivens, Tiana Gaudette, Garth Davies and Richard Frank Searching for Extremist Content Online Using the Dark Crawler and Sentiment Analysis. Ryan Scrivens, Tiana Gaudette, Garth Davies and Richard Frank. / Ryan Scrivens, Tiana Gaudette, Garth Davies and Richard Frank [Текст] // Methods of Criminology and Criminal Justice Research. —: Emerald Publishing, 2019. — С. 179-194.

8. New technology revealed to help fight terrorist content online / [Электронный ресурс] // Gov.uk : [сайт]. — URL:



<https://www.gov.uk/government/news/new-technology-revealed-to-help-fight-terrorist-content-online> (дата обращения: 31.07.2023).

9. Борьба с международным терроризмом и экстремизмом в центре внимания ШОС. В г. Душанбе состоялось Сопровождение генеральных прокуроров государств-членов ШОС / [Электронный ресурс] // Шанхайская организация сотрудничества. ШОС : [сайт]. — URL: <http://rus.sectsc.org/news/20180921/468260.html> (дата обращения: 31.07.2023).

10. Показатели преступности России / [Электронный ресурс] // Генеральная прокуратура Российской Федерации. Портал правовой статистики : [сайт]. — URL: http://crimestat.ru/offenses_chart (дата обращения: 31.07.2023).

11. Прокуратуры России и ОАЭ договорились о сотрудничестве в сфере борьбы с терроризмом и экстремизмом / [Электронный ресурс] // Интерфакс : [сайт]. — URL: <https://www.interfax-russia.ru/rossiya-i-mir/prokuratury-rossii-i-oe-dogovorilis-o-sotrudnichestve-v-sfere-borby-s-terrorizmom-i-ekstremizmom> (дата обращения: 31.07.2023).

12. О практике надзора в сфере противодействия экстремистской деятельности: в Бресте состоялось заседание Объединенной коллегии генеральных прокуратур Беларуси и России / [Электронный ресурс] // Генеральная прокуратура Республики Беларусь : [сайт]. — URL: <https://prokuratura.gov.by/ru/media/novosti/mezhdunarodnoe-sotrudnichestvo/o-praktike-nadzora-v/> (дата обращения: 31.07.2023).

13. Путин назвал экстремизм прямой угрозой единству России / [Электронный ресурс] // РБК : [сайт]. — URL: <https://www.rbc.ru/rbcfreenews/61bfbe379a794741a273aa8c> (дата обращения: 31.07.2023).

14. Бастрыкин предложил усилить мониторинг интернета на предмет экстремизма / [Электронный ресурс] // Russia Today : [сайт]. — URL:



ВОПРОСЫ РОССИЙСКОЙ ЮСТИЦИИ
ВЫПУСК № 26

<https://russian.rt.com/russia/news/948472-monitoring-bastrykin-internet>
обращения: 31.07.2023).

(дата