УДК 343.1

Булдыгеров Максим Николаевич, студент,
ФГАОУ ВО «Белгородский государственный национальный исследовательский университет»,
г. Белгород

Лукьянчикова Елена Федоровна,
к.ю.н., доцент кафедры уголовного права и процесса
ФГАОУ ВО «Белгородский государственный национальный исследовательский университет»,
г. Белгород

ПРОКУРОРСКИЙ НАДЗОР В СФЕРЕ ПРОТИВОДЕЙСТВИЯ РАСПРОСТРАНЕНИЮ ТЕРРОРИЗМА И ЭКСТРЕМИЗМА В СЕТИ ИНТЕРНЕТ
PROSECUTOR'S SUPERVISION IN THE SPHERE OF COUNTERING THE SPREAD OF TERRORISM AND EXTREMISM ON THE INTERNET

Аннотация: Данная статья освещает актуальные аспекты противодействия терроризму и экстремизму в контексте современной информационной среды, обращая внимание на роль и деятельность прокуратуры в этом процессе. В работе подробно рассматриваются различные методы использования Интернета террористическими организациями, включая создание виртуальных ресурсов, использование сервисов картографии, психологические атаки и финансовые операции по сбору средств. Особое внимание уделяется приоритетным задачам Генеральной прокуратуры Российской Федерации в области высокотехнологичного надзора, включая мониторинг информационных ресурсов, разработку законодательных инициатив и сотрудничество с правоохранительными органами. В заключение подчеркивается необходимость системного подхода к противодействию киберпреступности и важность сотрудничества между различными органами и институтами для обеспечения безопасности общества и предотвращения угроз национальной безопасности.

Abstract: This article highlights relevant aspects of countering terrorism and extremism in the context of the modern information environment, drawing attention to the role and activities of the prosecutor's office in this process. The scientific article examines in detail various methods of using the Internet by terrorist organisations, including the creation of virtual resources, the use of mapping services, psychological attacks and financial fundraising operations. Particular attention is paid to the priorities of the Russian Federation`s Office of the General Prosecutor in the area of high-tech oversight, including monitoring of information resources, development of legislative initiatives and co-operation with law enforcement agencies. In conclusion, the need for a systemic approach to countering cybercrime and the importance of co-operation between different offices and institutions to ensure the safety of society and prevent threats to national security are emphasised.

Ключевые слова: терроризм, экстремизм, сеть Интернет, киберпреступность, прокурорский надзор.

Keywords: terrorism, extremism, Internet, cybercrime, prosecutor's supervision.

В современном мире Интернет играет фундаментальную роль в повседневной жизни человека, занимая центральное положение в различных аспектах его деятельности. Основными сферами применения Интернета в двадцать первом веке являются: средства массовой информации (СМИ), доступ к интеллектуальной собственности, включая произведения искусства в различных формах, таких как: литература, кино, музыка, а также использование его в целях электронной коммерции и других смежных областях.

К несчастью, широкое распространения обретает и преступность в Интернете (киберпреступность) в различных странах и городах мира, причем Российская Федерация не остается в стороне в данном аспекте современных обстоятельств.

С ежедневным прогрессом информационных технологий возрастает масштаб возможностей для совершения преступлений в сети Интернет. Среди наиболее распространенных в России преступлений отмечаются: мошенничество, кража личных данных, а также атака на критическую инфраструктуру. Под критической инфраструктурой понимаются объекты, сети, службы и системы, нарушение работы которых может негативно сказаться на здоровье, безопасности и благосостоянии граждан страны [1, с. 2]. Цифровизация и расширение интернет-пространства привели к увеличению числа киберпреступлений, включая акты терроризма и экстремизма. Виртуальная среда предоставляет террористическим и экстремистским организациям площадку для пропаганды своих идеологий, вербовки новых членов и планирования атак.

Понятие терроризма закреплено в положениях п. 1 ст. 3 Федерального закона от 06 марта 2006 года № 35-ФЗ «О противодействии терроризму», в соответствии с которым под терроризмом понимается «идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий» [2]. В свою очередь экстремизм, основываясь на положениях Федерального закона «О противодействии экстремистской деятельности» от 25.07.2002 N 114-ФЗ, а также Указа Президента Российской Федерации от 29 мая 2020 г. № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года», определяется как общественно опасные деяния, совершаемые физическими и юридическими лицами по мотивам политической, идеологической, расовой, национальной, религиозной ненависти или вражды, а также объективно опасные деяния, способствующие возникновению или обострению межнациональных, межконфессиональных и межрелигиозных конфликтов [3; 4].

Террористические и экстремистские формирования используют Интернет в качестве мощного инструмента для манипулирования общественным мнением. Виртуальные ресурсы запрещенных в России организаций характеризуются высокой динамикой: они появляются неожиданно, постоянно преобразуются и моментально исчезают. Тем не менее, часто это исчезновение представляет собой лишь иллюзию, поскольку контент сохраняется неизменным, даже при изменении доменов и хостингов. В большинстве случаев эти сайты размещаются на серверах за рубежом, что затрудняет их закрытие на практике.

Содержание террористических ресурсов часто стандартизировано и включает различные элементы: исторический обзор деятельности организации, отчеты о выполненных операциях, ключевые события, биографии руководителей, изложение политических установок, критический анализ враждебных сил и актуальные события. В подаче информации террористические группы позиционируют себя как постоянно преследуемые и угнетаемые государством, представляя государственные органы в качестве подавляющей силы, которая ограничивает их свободу выражения и деятельности. Через такие действия террористы стремятся привлечь «сочувствующих» пользователей, выступая в роли защитников индивидуальных и политических свобод, в то время как государство изображается как агрессор, против которого необходимо бороться за права и свободы.

Использование сервисов картографии в качестве инструмента для планирования террористических деяний представляет собой значительную угрозу. Преступные группировки и террористические организации имеют возможность обращаться к данным о географическом

расположении объектов, инфраструктуре дорожного сообщения, населенных пунктах и прочей информации с целью более точного проектирования своих операций и избежания обнаружения со стороны правоохранительных органов.

Сервисы картографии, вроде «Google Maps» и «Яндекс.Карты», обеспечивают широкий доступ к детализированным картам и спутниковым изображениям, которые могут быть использованы для разведывательных целей и планирования операций. Например, террористические организации могут проводить изучение потенциальных объектов для атаки, разрабатывать маршруты побега, определять места для сокрытия оружия и т.д.

Для противодействия указанным угрозам необходимо тесное сотрудничество правоохранительных органов и интернет-провайдеров с целью наблюдения за подозрительной активностью и блокирования доступа к определенным данным или ресурсам. Важно также обеспечить профессиональное обучение специалистов в области кибербезопасности и продолжить развитие технологий для выявления и предотвращения террористических угроз в виртуальном пространстве.

Дополнительным методом использования Интернета террористическими организациями является создание виртуальных «энциклопедий», содержащих информацию об изготовлении оружия, сборке взрывных устройств, планировании террористических актов и прочих незаконных действиях. Помимо публичной пропаганды, террористы активно ведут психологические атаки через сеть, распространяя угрозы, вызывая панику и усиливая чувство страха и беспомощности. Это может включать распространение видеоматериалов о своих преступных действиях или создание ложных угроз о возможном взломе компьютерных систем аэропортов, военных объектов, фондовых бирж и прочих критически важных учреждений. Через Интернет террористические организации также проводят сбор средств для финансирования своих противоправных действий. Виртуальные платформы террористической агитации тщательно структурированы и организованы. За их функционированием внимательно следят специально обученные лица, обладающие необходимыми знаниями и качествами, что позволяет им воздействовать на аудиторию, не имеющую четко сформированного мировоззрения.

При проявлении распространения терроризма и экстремизма в сети Интернет особое внимание уделяется органам прокуратуры, которым поручается надзор за соблюдением законодательства в сфере информационных технологий. Законодательные основы деятельности органов прокуратуры по противодействию экстремизму в сети Интернет установлены в приказе Генпрокуратуры России от 21.03.2018 N 156 (ред. от 24.03.2023) «Об организации прокурорского надзора за исполнением законов о противодействии экстремистской деятельности» [5].

Прокурорский надзор в контексте противодействия распространению терроризма и экстремизма в сети Интернет играет существенную роль в обеспечении общественной безопасности и предотвращении угроз национальной безопасности. Начало формыПрокуроры осуществляют контроль за деятельностью организаций и граждан, осуществляющих пропаганду терроризма и экстремизма в сети Интернет, и принимают меры по пресечению их деятельности.

Прокуроры активно осуществляют мониторинг информационных ресурсов с целью выявления и блокирования материалов, содержащих экстремистские установки или призывы к совершению террористических актов. Кроме того, они осуществляют анализ соответствия деятельности организаций и граждан нормам законодательства, направленным на противодействие терроризму и экстремизму, и принимают меры по привлечению нарушителей к правовой ответственности.

Прокурорский надзор в данной сфере предполагает активное взаимодействие с правоохранительными структурами, специализированными органами и другими институтами с целью обмена информацией и согласования действий по противодействию угрозам терроризма и экстремизма в онлайн пространстве.

Исходя из вышеизложенного, прокурорский надзор является неотъемлемой составляющей обеспечения безопасности общества и превентивного противодействия угрозам национальной безопасности, обеспечивая соблюдение законности и защиту прав граждан от потенциальных террористических и экстремистских угроз.

Как отмечает А.А. Потапов, 17 июля 2020 года состоялось заседание высших должностных лиц правоохранительных органов Российской Федерации с целью координации их действий по рассмотрению вопроса «о состоянии работы правоохранительных и контролирующих органов по предупреждению, выявлению, пресечению и расследованию преступлений, связанных с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий, включая критическую информационную инфраструктуру Российской Федерации» [6, с. 293]. На данном заседании рассматривались проблемы, связанные с киберпреступной деятельностью и ее избыточной активностью на территории России. Было отмечено, что развитие новейших технологий все чаще выступает в качестве инструмента для осуществления широкого спектра преступлений, начиная от финансовых махинаций, связанных с кражей средств с банковских карт, и заканчивая угрозами безопасности государственной инфраструктуры и обеспечения ее защиты.

Прокуроры активно принимают участие в формулировании законодательных инициатив, направленных на ужесточение нормативных актов в области противодействия терроризму и экстремизму в сети Интернет, а также на усовершенствование механизмов реагирования на подобные проявления.

Также, основываясь на деятельности Генеральной прокуратуры Российской Федерации, можно выделить приоритетные задачи, которые Генпрокуратура рассматривает как наиболее эффективные для осуществления высокотехнологичного надзора:

1. участие в улучшении работы правоохранительных органов через обеспечение автоматизированной оценки;
2. внедрение современных информационных технологий в надзорную деятельность;
3. повышение скорости реагирования прокуратуры на нарушения закона и их предотвращение;
4. быстрый ответ на обращения граждан и юридических лиц;
5. гарантия получения объективной информации о законности и преступности;
6. обоснованное принятие решений на основе автоматизированного анализа нарушений;
7. предоставление рекомендаций для проверок с учетом выявленных закономерностей.

В заключение, в согласии с позицией А.А. Потапова, следует подчеркнуть, что для совершенствования деятельности прокуратуры в сфере киберпреступности необходимо сосредоточить внимание на противодействии преступлениям в онлайн среде. Прокурор должен предпринимать все возможные меры для обеспечения соблюдения законности в этой сфере, гарантировать наказание за нарушения, исключить безнаказанность преступников. Такой подход к прокурорскому контролю должен быть системным, учитывая динамику коммуникационных взаимоотношений в Интернете и сотрудничество с правоохранительными органами с целью предотвращения противоправной деятельности.

Список литературы:

1. Хлопов О.А. Проблемы кибербезопасности и защиты критической инфраструктуры // The Scientific Heritage. 2020. № 45-5 (45). URL: https://cyberleninka.ru/article/n/problemy-kiberbezopasnosti-i-zaschity-kriticheskoy-infrastruktury (дата обращения: 20.05.2024).

2. Федеральный закон «О противодействии терроризму» от 06.03.2006 № 35-ФЗ (последняя редакция) // КонсультантПлюс: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_58840/ (дата обращения: 20.05.2024).

3. Федеральный закон «О противодействии экстремистской деятельности» от 25.07.2002 № 114-ФЗ (последняя редакция) // КонсультантПлюс: [сайт]. –URL: https://www.consultant.ru/document/cons_doc_LAW_37867/ (дата обращения: 20.05.2024).

4. Указ Президента РФ от 29.05.2020 № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года» // КонсультантПлюс: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_353838/ (дата обращения: 20.05.2024).

5. Приказ Генпрокуратуры России от 21.03.2018 № 156 (ред. от 24.03.2023) «Об организации прокурорского надзора за исполнением законов о противодействии экстремистской деятельности» // КонсультантПлюс: [сайт]. – URL: https://www.consultant.ru/document/cons_doc_LAW_298172/ (дата обращения: 20.05.2024).

6. Потапов А.А. Прокурорский надзор за противодействием киберпреступности в информационно-телекоммуникационной сети Интернет / А. А. Потапов. – Текст: непосредственный // Молодой ученый. – 2020. – № 49 (339). – С. 292-297. – URL: https://moluch.ru/archive/339/76047/ (дата обращения: 20.05.2024).