

Дата поступления рукописи в редакцию: 20.06.2026 г.

DOI: 10.24412/2782-3849-2026-6-95-98

Дата принятия рукописи в печать: 25.06.2026 г.

КАНУБРИКОВ Виталий Алексеевич,

Начальник кафедры огневой подготовки Волгоградской академии МВД России, Кандидат юридических наук, доцент, полковник полиции,

e-mail: v.Kanubrikov@mail.ru

ВОЛОШИНА Олеся Павловна,

Старший преподаватель кафедры социально-гуманитарных дисциплин Брянского филиала Орловского юридического института МВД России имени В.В. Лукьянова,

e-mail: mail@law-books.ru

К ВОПРОСУ О ПРОТИВОДЕЙСТВИИ ДЕЯТЕЛЬНОСТИ ЭКСТРЕМИСТСКИХ ОРГАНИЗАЦИЙ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ: НЕЙТРАЛИЗАЦИЯ ДЕЗИНФОРМАЦИИ И ФАЛЬСИФИКАЦИИ

Аннотация. Автор в своей научной статье проводит исследование методов и способов борьбы с преступлениями, связанными с распространением недостоверной информации в сети Интернет, криминальными структурами и о применяемых правоохранительными органами эффективных мерах противодействия данному явлению в информационном пространстве.

Ключевые слова: дезинформация, противодействие, информация, сеть, анонимность, ответственность, криминальные структуры, правоохранительные органы, контроль, законодательство.

KANUBRIKOV Vitaly Alekseevich,

*Head of the Firearms Training Department Volgograd Academy of the Ministry of Internal Affairs of Russia
Candidate of Law, Associate Professor, Police Colonel*

VOLOSHINA Olesya Pavlovna,

*Senior Lecturer, Department of Social and Humanitarian Disciplines, Bryansk Branch of the Oryol Law
Institute of the Ministry of Internal Affairs of Russia named after V.V. Lukyanov*

ON THE ISSUE OF COUNTERING THE ACTIVITIES OF EXTREMIST ORGANIZATIONS IN THE INFORMATION SPACE: NEUTRALIZATION OF DISINFORMATION AND FALSIFICATION

Annotation. In this research article, the author examines the methods and means of combating crimes related to the dissemination of false information online, criminal organizations, and the effective measures law enforcement agencies employ to counter this phenomenon in the information space.

Key words: disinformation, counteraction, information, network, anonymity, responsibility, criminal organizations, law enforcement, control, legislation.

В условиях современных реалий динамично развивающееся информационное общество на базе информационно-телекоммуникационных технологий относится к общемировым тенденциям современности.

Сеть Интернет предоставляет широкие возможности, такие как общедоступность, высокая скорость передачи информации, независимость от местонахождения, анонимность и многие другие.

Такого вида привилегии включая и трудность в осуществлении контроля со стороны

органов правопорядка, привлекают внимание и криминальных структур, и они активно используют это в своей преступной деятельности, что позволяет им стать менее уязвимыми для правоохранительных органов.

Современные информационно-коммуникационные технологии значительно ускоряют циркуляцию данных, однако одновременно создают новые векторы угроз.

Злоумышленники эксплуатируют эти технологии для несанкционированного доступа к конфиденциальной информации пользователей и

ее последующей модификации.

Ключевая опасность заключается в целенаправленном распространении фальсифицированных сведений, направленных на причинение ущерба конкретным субъектам.

Масштабное распространение такой дезинформации способно дезориентировать общественность, подорвать легитимность государственных институтов и негативно сказаться на внешнеполитической стратегии государства.

Ответственность за преступления, в том числе связанные с распространением недостоверной информации, установлена статьями уголовного кодекса Российской Федерации.

Работники прокуратуры активно занимаются просвещением молодежи в образовательных учреждениях, объясняя им опасность ложных сообщений о террористических актах. Прежде чем говорить о мерах защиты, необходимо четко определить термин выражения - недостоверная общественно значимая информация.

Федеральный закон № 149 «Об информации, информационных технологиях и о защите информации», гласит, что первоочередной защите подлежит информация, которая может угрожать жизни и здоровью людей, их имуществу или общественной безопасности. Закон также предупреждает о возможности возникновения массовых протестов и беспорядков в результате распространения определенной информации.

Более того, получение злоумышленниками доступа к критически важным данным может привести к катастрофическим последствиям, включая уничтожение городской инфраструктуры, коммунальных и энергетических объектов, банков, промышленных предприятий и транспортных систем.

В Российской Федерации контроль над интернет-информацией осуществляют специализированные службы.

Их главная цель заключается в обеспечении противодействия умышленному распространению дезинформации и расследование киберпреступлений, то есть любых правонарушений, совершаемых в интернете или с использованием цифровых технологий.

Сотрудники этих служб занимаются выявлением, поиском и задержанием преступников, а также детальным изучением их поведения.

Особое внимание уделяется оперативному определению местонахождения тех, кто публикует угрожающую информацию, такую как террористические или экстремистские материалы, а также ложные сведения,

направленные на подрыв государственного строя России.

В практической деятельности применяется дифференцированное количество способов генерирования и распространения такой вредоносной информации.

Дезинформация, как правило, конструируется на основе подлинных сведений. Преступники используют стратегию искусного переплетения правды и вымысла, что затрудняет их дифференциацию.

Методология включает в себя представление неопровержимых фактов в начале сообщения, за которыми следует вводящая в заблуждение информация, часто расположенная в конце.

При этом сохраняется стилистическое единство с достоверной частью текста. Подобное смешение правды с ложью приводит к формированию ложных, но достоверных нарративов, которые искажают реальные события, адаптируя их под желаемую преступниками интерпретацию.

Процесс распространения фальсифицированных данных состоит из эксплуатации, подготовительной стадии и укрытия доказательств.

Социальные сети, обладая беспрецедентной скоростью и охватом, часто используются для распространения дезинформации.

Массовая аудитория, склонная к поверхностному восприятию информации и низкому уровню критического мышления, легко поддается ложным нарративам. Ежедневные миллионные просмотры и активное распространение контента через репосты позволяют злоумышленникам эффективно влиять на общественное сознание. Это влияние может проявляться в навязывании нехарактерных для российской действительности моделей поведения, искажении представлений о политических процессах и формировании негативного отношения к институтам власти и национальным ценностям.

Распространение дезинформации, как правило, ориентировано на определенные социальные группы, в первую очередь на молодежь, и служит для препятствования внешней политике России.

Источниками такой информации, новостей могут быть как частные лица и их агенты, так и зарубежные спецслужбы и организации.

Успех злоумышленников напрямую зависит от количества людей, подвергшихся воздействию дезинформации, поскольку их конечная цель заключается в том чтобы спровоцировать беспорядки в обществе и в

достижения этой цели создаются дополнительные материалы, призванные укрепить веру аудитории в ложную информацию и исключить сомнения.

В виду чего, с целью формирования доверия используются как полностью вымышленные, так и реальные, в том числе проверенные и надежные, источники.

В выше рассмотренном случае достоверные сведения могут быть искажены или представлены в выгодном для распространителей контексте, чтобы создать иллюзию подтверждения ложных новостей.

Вместе с тем такой метод как сокрытие следов, самый важный для злоумышленников, ведь им необходимо, чтобы спецслужбы не сумели точно определить, кто создал и распространил такую информацию.

Сомнительный источник может содержать другие новости, задача которых, отвлечь внимание от ключевого вопроса и вводная информация помогает скрыть следы и направляет не только общественность, но и правоохранительные органы на ложный след, так что теряется любая зацепка.

Не всегда злоумышленникам удается осуществить данный процесс.

Существует множество методов сокрыть следы, особенно преступники используют VPN, публикуют поддельные новости в интернет-группах, используют электронные устройства, которыми они не владеют, загружают с них данные и эти устройства удаляются сразу после работы.

Для выявления подделок необходимо использовать методы проверки фактов, для чего привлекаются эксперты, которые и занимаются проверкой представленных фактов на их достоверность.

Данные алгоритмы позволяют быстро выявить различия между поступающей информацией и проверенными источниками.

С целью сравнения фактов, можно отметить, что в нашей стране используется специальная организация, в цели которой и входит отслеживание и анализ фактов.

Также практикуется сверкой фактов и утверждений в статье, так и проверкой текста с языковой точки зрения, то есть, стиль, лингвистику, оценивают аргументированность автора и непосредственно проверяют достоверность фактов и в при необходимости эти организации передают запрошенную информацию в судебные органы.

Текстовые документы, статьи и небольшие заметки могут содержать ряд признаков, указывающих на то, что написанное в них не соответствует действительности, и это первый шаг проверочной работы.

В результате организация может сделать вывод о том, что информация является фальшивой, или выпустить предупреждение, если нет 100-процентной уверенности. Фальшивые новости представляют собой ложную информацию провокационного характера, содержащая диаметрально противоположные виды информации, такие как ложь и правда.

В виду чего информация становится более реалистичной и правдоподобной, так что ее трудно отличить от реальных фактов, особенно когда с ней сталкиваются граждане, которые не знают об этом, неподкованные в данной области и неосведомленные.

В отдельных случаях информация может быть реальной и содержащей в себе достоверные факты, однако эту же информацию возможно интерпретировать также можно вырвать с корыстными намерениями с выгодой для кого-либо.

Основная задача таких сообщений заключается в том, чтобы спровоцировать и последующем возбуждать, подрывать ценности и устои государства, его авторитетность, увеличивать дистанцию между

Главная цель процесса искажения информации заключается в том, чтобы захватить первые сроки новостных лент и максимально привлечь внимание аудитории, чтобы вменить гражданам недостоверную информацию, предварительно выдав ее за достоверную, чтобы они сосредоточились на них, постоянно размышляли, производя сильное впечатление, чтобы помнить об информации.

Преступники-террористы пытаются повлиять на общественность и внушить людям определенные навязчивые идеи и убеждения в отношении определенных идей.

Такие сообщения могут использоваться для создания ажиотажа, паники, провокаций и враждебной пропаганды, особенно терроризма и экстремизма, для дискредитации политиков и создания общественных волнений, дабы разрушить в подсознании граждан привычные устои и внушить веру в новые идеи.

Основная сложность в поиске преступников заключается в использовании современных технологий по типу VPN - такие технологии затрудняют вычисление реального адреса и местонахождения преступника, потому что преступники маскируют это и превращают свой IP-адрес в подделку, делая его привязанной к другому государству.

Однако алгоритмы, используемые правоохранительными органами, все равно позволяют вычислять и задерживать злоумышленников, и если те находятся на территории Российской Федерации, то

проблем с их задержанием не возникает, но если злоумышленник физически находится за границей, то необходимо заключить соглашение, что, конечно, отнимает много времени и не способствует скорейшему раскрытию преступления, ведь не все страны дают добро на выдачу преступника и отдачу его под стражу.

Отбор и фильтрация получаемой информации, а также ее проверка различными серверами перед отправкой публикации поможет уменьшить количество фальсификаций, но это технически трудно воплотить, в связи с чем основная роль в противодействии с исследуемыми правонарушениями отводится сотрудникам компетентных служб и подразделений.

В заключении проведенного исследования целесообразно отметить, что важной составляющей в системе противодействия идеологии экстремизма и терроризма в глобальном информационном пространстве должна стать информационно-пропагандистская работа, реализуемая в основном государственными службами во взаимодействии с другими организациями в сети Интернет.

Профилактическая деятельность, осуществляемая в целях формирования антитеррористического и антиэкстремистского сознания населения, должна основываться на принципах постоянства, систематичности, комплексности и к такой работе необходимо привлекать практических работников, занимающихся проблемами противодействия данным противоправным явлениям, научных деятелей, психологов, педагогов, студентов высших учебных заведений, общественных экспертов и представителей организаций, поскольку успешное решение данной проблемы требует координации усилий по дальнейшему совершенствованию технических средств и разработке новых методов информационного противодействия деятельности экстремистских организаций в информационном пространстве мирового масштаба.

Список литературы:

- [1] Сундиев И.Ю. Введение в оперативно-розыскную террологию: монография. М.: НИТИ-ДАНА: Закон и право, 2012. С. 191.
- [2] Ефремов М.И. Политический терроризм как форма этнического и религиозного экстремизма // Социология и социальная работа Вестник Нижегородского университета им. Н.И. Лобачевского. Серия Социальные науки, 2010.

№ 2 (18). С. 23-29.

[3] Петрянин А.В., Коннов И.А., Кузнецов М.В. Понятие, признаки и виды экстремизма: учебное пособие. Н. Новгород: НИУ РАНХиГС, 2019. С. 35-54.

[4] Федеральный закон от 25.07.2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» // СПС «КонсультантПлюс» (дата обращения: 07.04.2024).

[5] Зубалова О.А. Уголовно-правовые меры борьбы с организацией экстремистского сообщества: Дис. ... к.ю.н. Специальность 12.00.08 - уголовное право и криминология; уголовно-исполнительное право. Н. Новгород, 2013. С. 9, 22.

[6] Плотников В.В. Экстремизм как феномен современной социальной реальности: институциональные, системные и социоструктурные факторы: Автореф. дисс. ... д.социол.н. Специальность 22.00.04 - социальная структура, социальные институты и процессы. Краснодар, 2016.- С. 16.

[7] Стратегия противодействия экстремизму в Российской Федерации до 2025 года.

References:

[1] Sundiev I.Yu. Introduction to operational-search terrorology: monograph. M.: NITI-DANA: Law and Law, 2012. S. 191.

[2] Efremov M.I. Political terrorism as a form of ethnic and religious extremism//Sociology and social work Bulletin of Nizhny Novgorod University named after N.I. Lobachevsky. Social Sciences Series, 2010. № 2 (18). S. 23-29.

[3] Petryanin A.V., Konnov I.A., Kuznetsov M.V. Concept, signs and types of extremism: a textbook. N. Novgorod: NRU RANEP, 2019. S. 35-54.

[4] Federal Law No. 114-FZ of 25.07.2002 "On Countering Extremist Activities" //SPS ConsultantPlus "(date of appeal: 07.04.2024).

[5] O.A. Zubalova. Criminal law measures to combat the organization of an extremist community: Dis.... Ph.D. in 12.00.08 - criminal law and criminology; penal law. N. Novgorod, 2013. S. 9, 22.

[6] Plotnikov V.V. Extremism as a phenomenon of modern social reality: institutional, systemic and sociostructural factors: Autoref. diss.... Doctor of Social Sciences Specialty 22.00.04 - social structure, social institutions and processes. Krasnodar, 2016.- S. 16.

[7] Strategy to counter extremism in the Russian Federation until 2025.