О совершенствовании административных мер противодействия экстремизму

Алена Сергеевна Долженко
ФГКОУ ВО Дальневосточный юридический институт
Министерства внутренних дел Российской Федерации
имени И.Ф. Шилова, Владивостокский филиал
Россия, г. Владивосток, ул. Котельникова д. 21, 690087
E-mail: dolzhenko-74@internet.ru

Аннотация: в статье исследуется проблема противодействия информационному экстремизму в сети Интернет. Анализируются недостатки действующего административного законодательства и правоприменительной практики, в частности, проблемы с идентификацией правонарушителей, конфискацией орудий правонарушения и процессуальной фиксацией доказательств. Автором предлагается комплекс законодательных новелл, включающий введение в КоАП РФ новой меры обеспечения — «осмотра информации в сети Интернет», а также механизм судебной санкции на изъятие технических средств из жилища.

Ключевые слова: информационный экстремизм, сеть Интернет, административная ответственность, меры обеспечения производства, осмотр информации в сети Интернет, КоАП РФ, доказательства, правовые пробелы.

On improving administrative measures to combat extremism

Alyona Sergeevna Dolzhenko

Federal State Educational Institution of Higher Education Far Eastern Law Institute of the Ministry of Internal Affairs of the Russian Federation named after I.F. Shilov, Vladivostok branch

Russia, Vladivostok, Kotelnikova St., 21, 690087

Abstract: the article examines the problem of countering information extremism on the Internet. It analyzes the shortcomings of the current administrative legislation and law enforcement practice, particularly the problems with identifying offenders, confiscating the means of committing an offense, and procuring evidence. The author proposes a set of legislative innovations, including the introduction of a new enforcement measure in the Code of Administrative Offenses of the Russian Federation — «inspection of information on the Internet,» as well as a mechanism for judicial authorization to remove technical devices from a home..

Keywords: Information extremism, the Internet, administrative liability, measures to ensure production, inspection of information on the Internet, the Code of Administrative Offenses of the Russian Federation, evidence, legal gaps.

В настоящее время наблюдается резкое обострение проблемы распространения экстремистского контента в мировом информационном поле. Это делает критически важной задачу разработки и четкого нормативного закрепления эффективных административно-юрисдикционных механизмов для органов внутренних дел, направленных на выявление, предупреждение и пресечения деяний экстремистского характера. Необходимость таких мер подтверждается устойчивой тенденцией, подтвержденной практикой. Когда административные правонарушения перерастают в уголовные преступления.

Для противодействия этой негативной тенденции законодатель осуществляет принятие ряда нормативных актов. Центральное место среди них занимает Федеральный закон от 25 июля 2002 г.

№ 144-ФЗ «О противодействии экстремисткой деятельности» [1].

В научном обществе экстремизм принято разделять на насильственный и информационный [2, с. 40-48]. Первый имеет ограниченное влияние на широкие аудитории в силу своей локальности и необходимости прямого контакта с последователями. Второй, напротив, обладает повышенной общественной опасностью, чему способствует глобализация цифровых технологий, обеспечивающих анонимность, высокую скорость передачи данных, мультимедийность, низкую стоимость и легкость доступа к многомилионной аудитории [3, с. 37].

В эпоху повсеместной цифровизации насильственный экстремизм требует значительных ресурсов, тогда как государственные правоохранительные структуры разработали действенные методики его подавления. Таким образом, главную угрозу национальной безопасности представляет именно информационный экстремизм, использующий в качестве главного канала распространения Интернет.

Среди исследователей доминирует взгляд, что применение информационно-коммуникационных технологий стало неотъемлемой чертой экстремистской деятельности. В информационном обществе произошел сдвиг целей: вместо физического устранения политического деятеля достаточно добиться деструктивных последствий через манипуляции в киберпространстве [4, с. 187-192]. Глобальный характер Интернета представляет экстремистам обширную площадку для размещения противоправного контента через социальные сети, форумы и сайты, с использованием комплекса методов психологического воздействия — от публикации пропагандистских материалов до целенаправленной вербовки в личной переписке.

К специфическим чертам информационного экстремизма, способствующим его широкому распространению относят мгновенную скорость распространения информации, экономическую выгоду от использования технических средств, недостаточную законодательную проработку и нечеткость критериев привлечения к ответственности, доступность мультимедийного программного обеспечения, возможность анонимной публикации материалов, открытый доступ неограниченного числа пользователей и т.д.

Таким образом, интернет-экстремизм можно определить, как разновидность экстремистской деятельности, осуществляемую через противоправные действия физических и юридических лиц, которые пропагандируют идеологию нетерпимости и вражды и нацелены на дестабилизацию информационно-психологической и информационно-технической сфер общества путем создания, хранения и распространения в сети запрещенных материалов [5, с. 137].

Административная ответственность за правонарушения экстремисткой направленности закреплена несколькими статьями КоАП РФ, в частности: ст. ст. 13.15[1], 13.37[2], 20.3[3], 20.3.1[4], 20.29[5].

Производство по таким делам представляет собой административно-юрисдикционный процесс, регулируемый КоАП РФ. Его главной задачей является всестороннее и объективное выяснение всех обстоятельств инцидента. Для этого законодатель устанавливает систему мер принуждения, применяемых в строго процессуальном порядке (гл. 27 КоАП РФ).

Согласно классификации А.В. Коркина, эти меры делятся на применяемые к физическим лицам, к юридическим лицам и универсальные [6, с. 37-41]. Все они потенциально могут быть использованы в контексте интернет-экстремизма.

Специфика цифровой среды создает трудности в обнаружении и документировании правонарушений. Установление личности правонарушителя требует мониторинга сетевого контента и направления официальных запросов владельцу интернет ресурса для получения IP-адреса или провайдеру для идентификации абонента, которому был назначен IP-адрес на момент совершения

правонарушения. Если использовалась беспроводная сеть, идентификация возможна по MAC- или EMEI- адресу устройства.

После установления личности возникает проблемы с обеспечением производства, в частности, изъятия орудия правонарушения (компьютерной техники), которое часто находится в жилом помещении. Действующим законодательством не предусмотрен механизм принудительного изъятия орудия правонарушения в жилом помещении в связи с совершением административного правонарушения. Для устранения этого пробела предлагается внести поправки в част 3 статьи 15 Федерального закона «О полиции», предусмотрев получение судебного решения на обследование жилого помещения и изъятия орудий правонарушений.

Вторая группа проблем связана с доказыванием. Информацию в сети удалить легко, что требует ее оперативной и юридической фиксации. Единственно применимой мерой для осмотра интернет-контента является осмотр помещений и территорий, принадлежащих юридическому лицу (ст. 27.8 КоАП РФ). Однако ее использование сопряжено с риском признания доказательств недопустимыми из-за неочевидности отнесения веб-страницы к объекту осмотра в смысле ст. 27.8 КоАП РФ, отсутствия законодательно утвержденных требований к протоколу осмотра информации в сети Интернет и ориентации нормы на юридических лиц и индивидуальных предпринимателей, что не позволяет применять ее к сайтам, принадлежащим физическим лицам.

Суды часто не признают скриншоты, сделанные сотрудниками, допустимыми доказательствами, отдавая предпочтение нотариально удостоверенным осмотрам [7, с. 92-98]. В связи с этим целесообразно законодательно закрепить в КоАП РФ специальную меру обеспечения — «Осмотр информации в сети Интернет», детализировав его понятие, основание, процедуру проведения и требования к протоколу. Можно предложить следующий алгоритм такого процессуального действия:

— проведение в присутствии двух понятых или с обязательной видеофиксацией;

— фиксация в протоколе данных о техническом устройстве, сетевом подключении (IP-адрес, провайдер), доменном имени, администраторе сайта и содержании просматриваемой информации;

— приложение к материалам дела распечаток скриншотов на бумаге формата А4, заверенных печатью и подписью должностного лица;

— использование лицензионного программного обеспечения для определения IP-адреса и доменного имени с отражением сведений о программе в протоколе.

Не менее актуален вопрос об изъятии цифровых носителей, содержащих экстремистские материалы. В качестве альтернативы, позволяющей сохранить право собственности, предлагается дополнить статью 4.1 КоАП РФ положением, обязывающим суд возлагать на виновного обязанность удалить запрещенную информацию со своих устройств под надзором правоохранительных органов.

Цифровая трансформация общества обусловила рост информационного экстремизма, который превосходит насильственный по масштабу негативного воздействия. Для противодействия ему необходима разработка четких административных процедур и унификация правоприменительной практики. Меры обеспечения производства по административным делам являются легальным инструментом принуждения, используемым для нормального ведения процесса. Их результативное применение требует отлаженного межведомственного взаимодействия. Ключевым элементом доказывания выступает осмотр информации в сети Интернет, который следует законодательно ввести в КоАП РФ в качестве самостоятельной меры обеспечения. Реализация предложенных изменений позволит усилить эффективность административно-правового противодействия распространению экстремизма в глобальной сети.

Литература:

1. Федеральный закон от 25.07.2002 N 114-ФЗ (ред. от 23.07.2025) «О противодействии экстремистской деятельности» (с изм. и доп., вступ. в силу с 01.09.2025).

2. Гаджимурадова, Г. И. Информационные технологии и противодействие различным видам экстремизма в эпоху глобализации / Г. И. Гаджимурадова // Научный результат. Социология и управление. — 2021. — Т. 7, № 2. — С. 40-48.

3. Мкртычан А.А. Влияние средств массовой информации на психологические последствия терроризма : автореф. дис. ... канд. психол. наук. М., 2012. С. 37.

4. Старосветский Е.А. Экстремизм в современном российском обществе // Научные ведомости Белгород. гос. ун-та. 2008. № 5. С. 187–192.

5. Глухарев Д.С. Противодействие экстремизму в современном медиапространстве // Вестник Юж.-Урал. гос. ун-та. 2012. № 10. С. 137.

6. Коркин А.В. Процессуальность как признак мер обеспечения производства по делам об административных правонарушениях // Юридическая наука и правоохранительная практика. 2017. № 4 (42). С. 37–41.

7. Мурзина Л.И., Толоконникова А.С. Правовые проблемы осмотра места совершения административного правонарушения // Наука. Общество. Государство. 2019. № 2 (26). С. 92–98.

References:

1. Federal Law No. 114-FZ of July 25, 2002 (as amended on July 23, 2025) «On Countering Extremist Activities» (as amended and supplemented, intro. effective from 09/01/2025).

2. Gadzhimuradova, G. I. Information technologies and countering various types of extremism in the era of globalization / G. I. Gadzhimuradova // Scientific result. Sociology and management. — 2021. — Vol. 7, No. 2. — Pp. 40-48.

3. Mkrtichan A.A. Influence of Mass Media on the Psychological Consequences of Terrorism: Abstract of Dissertation. ... Candidate of Psychology. Moscow, 2012. P. 37.

4. Starosvetsky E.A. Extremism in Contemporary Russian Society // Scientific Bulletin of Belgorod State University. 2008. No.

5. Pp. 187–192. 5. Glukharev D.S. Counteraction to Extremism in the Modern Media Space // Bulletin of the South-Ural State University. 2012. No. 10. P. 137.

6. Korkin A.V. Procedural Aspects of Administrative Offenses // Legal Science and Law Enforcement Practice. 2017. No. 4 (42). Pp. 37–41.

7. Murzina L.I., Tolokonnikova A.S. Legal Issues of Inspecting the Scene of an Administrative Offense // Nauka. Obshchestvo. Gosudarstvo. 2019. No. 2 (26). Pp. 92–98.

Дополнительная информация об авторе:

А.С. Долженко — старший преподаватель кафедры оперативно-разыскной и административной деятельности ВФ ФГКОУ ВО «ДВЮИ МВД России имени И.Ф. Шилова».

Ссылки:

1. Злоупотребление свободой массовой информации.

2. Распространение владельцем аудиовизуального сервиса информации, содержащей публичные призывы к осуществлению террористической деятельности, материалов, публично оправдывающих терроризм, или других материалов, призывающих к осуществлению экстремистской

деятельности либо обосновывающих или оправдывающих необходимость осуществления такой деятельности.

3. Пропаганда либо публичное демонстрирование нацистской атрибутики или символики, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены федеральными законами.

4. Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства.

5. Производство и распространение экстремистских материалов.