Научная статья
УДК 343.85:343.34:004.77(470+476)

Ильфат Давлетнурович Бадамшин[1], Марина Владимировна Савич[2]
[1] Уфимский юридический институт МВД России, Уфа, Россия, Badam02@mail.ru
[2] Учреждение образования «Институт повышения квалификации и переподготовки Следственного комитета Республики Беларусь», Минск, Республика Беларусь, Savich_marina78@mail.ru

ПРОТИВОДЕЙСТВИЕ ИДЕОЛОГИИ ТЕРРОРИЗМА И ЭКСТРЕМИЗМА В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОМ ПРОСТРАНСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ И РЕСПУБЛИКИ БЕЛАРУСЬ

Аннотация. Повсеместное использование цифровых технологий и коммуникаций в различных отраслях и сферах общественной жизни стало доминирующим фактором для создания единого информационного пространства, способного воздействовать на массовое сознание и формирование определенных социальных групп. В то же время, к сожалению, прогресс в сфере IT инициировал распространение идеологии терроризма и экстремизма.

Преступления террористического и экстремистского характера занимают особое место в структуре общей преступности. На протяжении последних лет в динамике данного показателя не прослеживается устойчивых тенденций к снижению. Рассматриваемые преступления всегда были и остаются общественно опасными, их совершение сопровождается неизгладимыми социальными потрясениями и последствиями, колоссальными материальными затратами, а также, что более всего страшно, невосполнимыми потерями человеческих жизней.

В контексте современной трансформации общественных отношений изучение проблемных аспектов противодействия идеологии терроризма и экстремизма, включая их актуальные проявления через информационно-телекоммуникационные технологии, в частности сеть Интернет, представляется своевременным и актуальным.

Ключевые слова: терроризм, идеология, негативный контент, деструкция, противодействие, информационно-телекоммуникационные сети, сеть Интернет, социальные сети

Для цитирования: Бадамшин И. Д., Савич М. В. Противодействие идеологии терроризма и экстремизма в информационно-телекоммуникационном пространстве Российской Федерации и Республики Беларусь // Общество, право, государственность: ретроспектива и перспектива. 2025. № 4 (24). С. 43–52.

Original article

Ilfat D. Badamshin[1], Marina V. Savich[2]
[1] Ufa Law Institute of the Ministry of Internal Affairs of Russia, Ufa, Russia, Badam02@mail.ru
[2] Educational Institution "Institute for Advanced Training and Retraining of the Investigative Committee of the Republic of Belarus", Minsk, Republic of Belarus, Savich_marina78@mail.ru

COUNTERACTING THE IDEOLOGY OF TERRORISM AND EXTREMISM IN THE INFORMATION AND TELECOMMUNICATIONS SPACE OF THE RUSSIAN FEDERATION AND THE REPUBLIC OF BELARUS

Abstract. The widespread use of digital technologies and communications in various industries and spheres of public life has become a dominant factor in the creation of a single information space capable of influencing mass consciousness and the formation of certain social groups. At the same time, unfortunately, progress in the IT sector has become one of the fundamental factors initiating the spread of propaganda of the ideology of terrorism and extremism.

Terrorist and extremist crimes occupy a special place in the structure of general crime. Over the past few years, there have been no stable downward trends in the dynamics of this indicator. The crimes in question have always been and remain socially dangerous, their commission is accompanied by indelible social upheavals and consequences, colossal material costs, and, what is most frightening, irreparable losses of human lives.

In the context of the modern transformation of social relations, the study of problematic aspects of counteracting the ideology of terrorism and extremism, including their current manifestations through information and telecommunication technologies, in particular the Internet, seems timely and relevant.

Keywords: terrorism, ideology, negative content, destruction, counteraction, information and telecommunication networks, Internet, social networks

For citation: Badamshin I. D., Savich M. V. Counteracting the ideology of terrorism and extremism in the information and telecommunications space of the Russian Federation and the Republic of Belarus // Society, law, statehood: retrospective and perspective. 2025. No. 4 (24). P. 43–52. (In Russ.)

Введение

За последние пять лет только на территории Российской Федерации было совершено более 19 000 преступлений террористического характера и экстремистской направленности. Так, в 2020 г. это 2342 и 833 преступления соответственно, в 2021 – 2136 и 1057, в 2022 – 2233 и 1566, в 2023 – 2382 и 1340, в 2024 – 3714 и 1719, в 2025 (по состоянию на май) – 2545 и 941[1]. Статистические данные за последние годы свидетельствуют о тенденции роста рассматриваемых преступлений.

Относительно преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, за аналогичный период времени их количество увеличилось на 66,6 %, с 510 396 до 765 365. В 2025 г. (по состоянию на май) совершено 308 119 преступлений[2].

Деятельность по предупреждению преступлений террористического характера целесообразно рассматривать как важный компонент всей системы противодействия указанному деструктивному социальному явлению [1, с. 185–197]. Должная ее настройка, без сомнения, будет способствовать снижению количества таких преступлений, что в конечном итоге повысит общую общественную безопасность граждан, общества и государства в целом.

На протяжении последнего столетия средства массовой информации формировали и продолжают формировать общественное восприятие ключевых событий, влияя на ход истории и принятие решений. Изучение многочисленных периодических изданий, что могли себе позволить многие, являлось практически единственным источником удовлетворения в той или иной степени информационного «голода» как на территории бывшего СССР, так и практически во всем мире.

Особенностью современной действительности является повсеместное внедрение в жизнь практически каждого человека более потенциально мощного инструмента – глобальной информационно-телекоммуникационной сети, в том числе сети Интернет во всем многообразии ее представления. Так, агентство We Are Social и Meltwater опубликовали ежегодное исследование состояния сферы диджитал, согласно которому к началу 2025 г. общее количество использующих Интернет составило 67,9 % населения земного шара – 5,56 млрд человек, увеличившись за год на 136 млн (2,5 %). Количество пользователей социальных се-

[1] Краткая характеристика состояния преступности в Российской Федерации // МВД России. URL: https://мвд.рф/reports?ysclid=mf9da548yp65454642 (дата обращения: 02.07.2025).

[2] Там же.

тей выросло более чем на 4,1 % и насчитывает 5,24 млрд – это 63,9 % от общей численности населения мира[1].

Относительно Российской Федерации отметим, что если в 2021 г. Интернетом пользовалось 129,8 млн человек, что составляет 89 % от общего количества населения России[2], то уже по состоянию на январь 2025 г. количество интернет-пользователей составило 133 млн человек, а уровень проникновения Интернета – 92,2 %. Пользователей социальных сетей насчитывалось 106 млн (73,4 % от общей численности населения)[3].

Как нам представляется, приведенные данные фактически являются несколько заниженными в связи с наличием официальной возможности самостоятельной регистрации в социальных сетях только при достижении тринадцатилетнего или же шестнадцатилетнего возраста (Telegram, «ВКонтакте», «Дзен», «Одноклассники», RuTube, YouTube, TikTok). Учитывая, что доступ к информации в сети Интернет осуществляется даже детьми начиная с трехлетнего возраста, преимущественно с целью потребления развлекательного контента, они используют учетные записи старших членов семьи (братьев, сестер или родителей), тем самым фактически становясь активными пользователями цифрового пространства. В результате их активность в цифровой среде не фиксируется в статистике.

Среднестатистический российский пользователь проводит в Интернете каждый день более семи часов, то есть более 40 % бодрствования[4].

По данным исследования Brand Analytics «Социальные сети в России: цифры и тренды», в конце 2021 г. активных авторов соцмедиа насчитывалось 66,4 млн. Проникновение Интернета составило 85 %. Более трети россиян, используя одну или несколько соцсетей, писали хотя бы один пост в месяц, а все вместе – 1,1 млрд публичных сообщений[5].

По состоянию на март 2025 г. число активных авторов в социальных медиа в России составило 83,8 млн. Авторы написали 1,93 млрд публичных сообщений – постов, репостов и комментариев. По сравнению с мартом 2024 г. наблюдается значительный прирост активных авторов (+22,5 %) и незначительный прирост создаваемого ими контента (+4,3 %)[6].

Динамика роста интернет-пользователей наблюдается и в Республике Беларусь. Удельный вес населения (в возрасте 6–72 лет), использующего сеть Интернет по территории Республики Беларусь, составлял в 2021 г. 86,9 %, в 2024 г. – 94,3 %. При этом удельный вес населения (в возрасте 6–72 лет), использующего сеть Интернет ежедневно, в 2021 г. был на уровне 74,1 %, в 2024 г. – 86,0 %[7].

Методы

В ходе научной работы был применен широкий методологический инструментарий. Обобщение, дедукция, индукция, син-

[1] Kemp S. Digital 2025: global overview report // DataReportal. URL: https://datareportal.com/reports/digital-2025-global-overview-report (дата обращения: 02.07.2025).

[2] Отчет «Digital 2022 Russian Federation» – Цифровые тенденции в России в 2022 году // CPA.RIP. URL: https://cpa.rip/stati/digital-2022-russian-federation/ (дата обращения: 02.07.2025).

[3] Тимонова А. Статистика интернета и социальных сетей России на 2025 год: главные тренды и цифры // WebCanape. URL: https://www.web-canape.ru/business/statistika-interneta-i-socialnyh-setej-rossii-na-2025-god-glavnye-trendy-i-cifry/?ysclid=md63045m36151600933#2 (дата обращения: 02.07.2025).

[4] Глава ИРИ рассказал, сколько времени россияне проводят в интернете // РИА НОВОСТИ. URL: https://ria.ru/20250619/internet-2024004238.html?ysclid=md6xllxt9z787417897 (дата обращения: 02.07.2025).

[5] Чёрный В. Социальные сети в России: цифры и тренды, осень 2021 // Brand Analytics. URL: https://br-analytics.ru/blog/social-media-russia-2021 (дата обращения: 02.07.2025).

[6] Социальные сети в России: цифры и тренды, весна 2025 // COSSA. URL: https://www.cossa.ru/Brand_Analytics/341164/?ysclid=md6xvz34pt567286741 (дата обращения: 02.07.2025).

[7] Интерактивная информационно-аналитическая система распространения официальной статистической информации // Национальный статистический комитет Республики Беларусь. URL: https://dataportal.belstat.gov.by/osids/rubric-info/1063268 (дата обращения: 10.07.2025).

тез, анализ и сравнение составили основу общенаучного подхода. Исследование социально-правовой реальности дополнительно опиралось на специализированные методы: системно-структурный, формально-юридический, а также моделирование.

Результаты

В условиях современной действительности совокупность применяемых и перспективных информационных технологий, которые все шире внедряются в повседневную жизнь общества, к сожалению, является фактором, оказывающим значительное влияние как на позитивные, так и на негативные общественные характеристики. К настоящему моменту подтверждена прямая пропорциональная зависимость числа преступлений, совершаемых в киберпространстве, от количества пользователей сетей. Также непосредственное использование средств информационного воздействия нашло большой практический интерес у террористических и экстремистских организаций.

При этом мы согласны, что с понятием терроризма в информационно-телекоммуникационных системах и сетях связано множество сложностей [2, с. 471]. Во-первых, отсутствует методика однозначного определения числа пострадавших от насилия и возможность полноценного, гарантированного удостоверения личности их инициатора ввиду полной виртуализации и анонимности. В данном контексте большинство преступников, совершивших рассматриваемые противоправные акты в сетях, не отождествляются именно с личностью террористов или экстремистов. Во-вторых, толкование терроризма опосредует его восприятие не как разовой акции какой-либо группы, связанной с определенного рода манифестной деятельностью, а как комплекс действий, имеющих в своем основном содержании разрушающую или уничтожающую активность в отношении выбранной цели. Данное действие совершается целенаправленно, динамично и, возможно, на некой регулярной основе.

Таким образом, для современных реалий характерно смещение акцента со среды совершения терроризма в сферу массмедиа и социальных сетей, где реализуется различного рода деструктивный контент идеологического, насильственного, политического или иного содержания, который ориентирован не на уничтожение, а скорее на всеобщность и значимость своего информационного освещения [3, с. 104].

Еще раз подчеркнем, что важнейшими объективными составляющими виртуальной реальности являются ее глобальность и интерактивность. Интернет не признает условностей времени, территорий, возраста, расы и пола. В независимости от данных критериев он оказывает преимущественное влияние на формирование ценностно ориентированных смысловых установок личности. В настоящее время данным ресурсом активно пользуются и носители радикальных мировоззрений, объединяющиеся на новейшей идеологической основе. Неизбежным воплощением ее, как правило, всегда выступает терроризм.

Для того чтобы государство и общество могли противостоять этой экспансии, целесообразно активно использовать механизмы наиболее эффективных методов и технологий противодействия идеологии терроризма и экстремизма в информационном поле Интернета.

По нашему мнению, эффективно противодействовать рассматриваемому негативному контенту необходимо комплексно, с учетом реализации трех основных направлений: организационно-правового, идеологического и технического.

Организационно-правовое направление.

Изначально в связи с тем, что данное явление имеет международный характер и не знает границ, его содержанием является становление, развитие и укрепление международных отношений в сфере обеспечения информационной безопасности от всевозможных угроз в Глобальной сети между государствами, правоохранительными органами, службами и международными организациями. Обмен знаниями и опытом в борьбе с радикальной идеологией, различными ее проявлениями и практиками мониторинга информационных ресурсов, проведения экс-

пертиз может оказать существенное влияние на положение дел в данной сфере. В этом вопросе способствовало бы принятие международных законов об информационной безопасности и борьбе с терроризмом в виртуальном пространстве. При этом отметим, что стратегическое значение имеет наличие прямого взаимодействия между государствами по обмену информацией об угрозах, признаках, фактах, способах и средствах использования информационно-телекоммуникационных систем в данных противоправных целях [4, с. 66].

Во-вторых, на постоянной основе необходимо осуществлять непрерывное совершенствование действуюшего законодательства, касающегося правил обращения с информационными цифровыми источниками, строгого регламентирования прав, а также ответственности пользователей, проявляющих активность в открытых глобальных сетях.

В-третьих, следует осознать в вопросах борьбы с идеологией терроризма и экстремизма важность роли привлечения к ней общественных организаций, этнокультурных и религиозных движений и обществ. Необходимо обратить внимание и на то, что до сих пор мало задействованы в сфере противодействия терроризму возможности ветеранских организаций и патриотических движений. Особый акцент здесь следует поставить на их полезности, большом перспективном потенциале и высокой эффективности.

В-четвертых, в качестве методов противодействия можно рассматривать историческую востребованность:

а) сотрудничества государственных органов и структур, занимающихся вопросами противодействия терроризму и обеспечением информационной безопасности;

б) неотвратимости применения жестких санкционных мер в отношении лиц, являющихся идеологами или распространителями террористических и экстремистских взглядов и идей, а также самих лиц, непосредственно причастных к кибертерроризму.

Идеологическое направление.

Сознание любого человека на интуитивном уровне сопряжено с пониманием явления терроризма с точки зрения воздействия на основы безопасности [5, с. 267]. Идеология террора сама по себе и уж тем более непосредственное совершение террористических актов, с одной стороны, формируют и усиливают в обществе чувство обеспокоенности, паники, страха, трансформируют все существующие ценности, обесценивают человеческую жизнь, с другой стороны, приводят к ограничению или полной невозможности реализации со стороны государства основополагающих гарантий прав и свобод личности.

В этой связи идеологическое направление противодействия терроризму и экстремизму на государственном уровне должно осуществляться:

а) активным проведением информационно-пропагандистских мероприятий с максимально широким охватом потенциальной аудитории, влияющих на антитеррористические ценностные установки населения;

б) созданием сети информационных ресурсов, обеспечивающих пользователей своевременной, объективной и достоверной информацией о террористической угрозе и негативном влиянии радикальных религиозных, экстремистских и террористических организаций.

Во-первых, как представляется, в современных реалиях наиболее оптимальными и функциональными платформами для осуществления противодействия идеологии терроризма и экстремизма в рамках просвещения и освещения являются блогосфера и социальные сети. Это позволит рассчитывать на максимальный охват аудитории.

Их потенциальный функционал и основное преимущество – возможность прямого (online) обмена знаниями и мнениями между пользователями, обмена теоретическими наработками, практическим опытом между профессионалами медийного сектора, а также развитие конструктивного диалога между средствами массовой информации и другими заинтересованными секторами Интернета.

На данных информационных ресурсах, в блогах и на форумах целенаправленно долж-

на освещаться и обсуждаться тематика различного содержания. В частности, это может быть: о неприятии идеологии терроризма и религиозно-политического экстремизма; об уважительном отношении к традиционным религиям; о высказываниях духовных лидеров основных религиозных конфессий. Безусловно, должны размещаться и материалы деятельности федеральных органов исполнительной власти в сфере противодействия терроризму и экстремизму, Национального антитеррористического комитета, Антитеррористического центра государств – участников Содружества Независимых Государств, а также информация о научно-теоретических, информационно-пропагандистских мероприятиях антитеррористической направленности в России и за рубежом.

Во-вторых, в целях противодействия идеологии терроризма и экстремизма в сети Интернет необходимо использовать технологии контрпропаганды. Приоритетным ее направлением должна стать совокупность способов воздействия на целевые группы населения для формирования ценностно-смысловых установок, ориентированных на антитеррористические, толерантные формы сознания и поведения. При этом важно учитывать их ресурсность и содержательно-информационные компоненты, составляющие познавательную основу, соответствие заявленным целям, адресность различных групп населения с учетом их возраста, гендерных особенностей, а также социальных параметров, информационную новизну, этническую целесообразность и т. д.[1]

К разряду рассматриваемой деятельности отнесем и создание так называемого отрицательного фона, то есть проведение массированных целенаправленных кампаний по дискредитации террористических и экстремистских организаций. Главная их цель состоит в нивелировании ощущений престижа и избранности причастных к подобным группировкам. В частности, данный подход хорошо зарекомендовал себя в вопросах снятия ореолов романтизма и героизма у новичков и сочувствующих [6, с. 82].

Следующий этап, который необходимо реализовать во всем информационном пространстве, – нейтрализация влияния путем компрометации и последующей дискредитации лидеров и активных участников террористических организаций. Обнародование данных фактов (жадности, ошибок, замалчивания) минимизирует привлекательность таких организаций, влечет за собой их разобщение, снижает качество и активность противоправной групповой деятельности, заставляя их пребывать в непрерывном стрессе, панике и ощущать серьезный прессинг [7, с. 241].

В-третьих, одним из основных способов противодействия идеологии терроризма и экстремизма в коммуникационных сетях является убеждение. Его эффективность может быть достигнута путем использования технологии прямого воздействия на ценностные ориентации и мировоззренческие оценки пользователей информационных контентов с применением рациональных аргументов, логики, аналитических материалов, конкретных целевых примеров и др. В частности, следует формировать в социуме устойчивое неприятие самой идеологии терроризма и экстремизма, в целях чего целесообразно использовать аргументации и контраргументации, которые при правильном их применении будут непосредственно способствовать достижению убеждающего эффекта [8, с. 202].

Отметим, что аргументация в контексте убеждения – это не демонстрация собственной правоты, достижений и значимости, а средство информационного (интеллектуального) воздействия на позицию оппонента, где в целях достижения успеха необходимо осуществлять взаимодействие в рамках его логики. В данном случае увеличивается вероятность построения конструктивной двусторонней взаимосвязи, когда оппонент

[1] Экстремизм и терроризм в Интернете (памятка) // Посреди России. URL: https://posredi.ru/category/antiterror (дата обращения: 03.07.2025).

понимает и воспринимает для себя возможность принятия обоюдного решения.

Контраргументация – выдвижение собственных доводов для объективного опровержения аргументов и выводов оппонента. Констатация аргументов и (или) контраргументов, приемы их выдвижения и построения в информационно-телекоммуникационной сети, в том числе в сети Интернет, должны осуществляться корректно, а также целиком и полностью быть ориентированы на оппонентов (пользователей), в ходе виртуального диалога с которыми необходимо оперировать воспринимаемыми и понятными для них терминами и формулировками, опираться на признаваемые ими критерии и достоверные для них аргументы, учитывать их жизненный опыт, возраст, интересы, цели и мотивы. Принципиально важно использовать только достоверную информацию, а также должным образом учитывать и следить в процессе текстовой переписки (дискуссии) за соблюдением выбранной тактики поведения и манерой общения. Особое внимание следует уделять используемым в тексте формулировкам, оборотам речи и лексикону в связи с невозможностью последующей, после ознакомления с ним оппонента, их корректировки или удаления.

Техническое направление.

Деятельность по противодействию в рамках реализации указанного направления может осуществляться в виде ограничения доступа к определенным материалам. Ограничительные меры в сети Интернет по блокировке информации могут осуществляться путем:

а) запрета доступа конкретным лицам или конкретным компьютерам в Интернет в целом;

б) сокрытия результатов поиска в поисковой системе;

в) запрета доступа к веб-сайтам с определенными, заранее известными адресами;

г) дозирования информации, подачи ее в усеченном варианте;

д) нарушения логики (структуры) информационного контента;

е) усложнения доступа к определенной информации (принудительное снижение скорости соединения для предотвращения скачивания и получения материалов).

Подобные меры могут быть реализованы как правоохранительными органами, так и специальными службами контроля и мониторинга. Выявление противоправного контента деструктивного содержания и последующее информирование вышеуказанных субъектов воздействия – это в том числе задача гражданского общества.

Характеризуя кибертерроризм, отметим, что в зависимости от преследуемых определенными субъектами целей это не только осуществляемое различным инструментарием деструктивное воздействие, но и непосредственно несанкционированный доступ к различной информации, как правило, конфиденциальной или даже секретной, обрабатываемой с использованием средств вычислительной техники, а также к аппаратуре, предназначенной для передачи данных, посягательство на информационные системы и их элементы, позволяющие в нее проникнуть.

Данные особенности приобретают в настоящее время все большую остроту и могут детерминировать увеличение общего количества такого характера вызовов, рисков и угроз. В качестве примера можно привести не так давно пройденный нами период пандемии, когда многие структуры, организации и предприятия, как государственные, общественные, так и коммерческие, были вынуждены принять неординарные меры и впервые в истории перевести своих сотрудников на удаленную работу. При этом для продолжения нормального работоспособного функционирования они предоставляли им удаленный доступ к информационным системам. И если ее организация и осуществление последующего взаимодействия не представляла технических трудностей, то проблема обеспечения безопасности передаваемых данных резко обострилась.

Практика показала, что не все субъекты были готовы гарантировать защищенность своей информации, прежде всего потому, что у большинства из них такой проблемы раньше не существовало в связи с отсутстви-

ем необходимости выхода в общедоступные сети. Соответственно, не все они оказались способными обеспечить безопасные соединения, а лица, получившие удаленный доступ и работающие с данной информацией, не в полной мере владели навыками ее защиты и обеспечения безопасности, вследствие чего резко возросло количество уязвимостей различных информационных ресурсов и систем.

Еще одна проблема может быть связана со спам-рассылками. Фишинговые письма могут привести к несанкционированному доступу к системе, когда пользователь просто переходит по незнакомой ссылке. В данном случае защитой может стать только запрет на переход по ссылкам.

В целом же важно наличие специалиста, отвечающего за безопасность информационной системы, использующейся в различных структурах, организациях и предприятиях, для качественного проведения ее мониторинга, решения проблем, возникающих при использовании коммуникационных сетей, для установки фильтров на нежелательные ресурсы, организации помощи и оперативного принятия решений в экстренных ситуациях, связанных с несанкционированным доступом [9, с. 101].

Сегодня и в ближайшей перспективе принципиально важно, помимо основной защиты компьютерных устройств с помощью разнообразных технических программных средств от несанкционированного доступа и иных противоправных операций, проводить организационные, методические и обучающие мероприятия непосредственно с легальными пользователями информационных систем по повышению уровня их компьютерной грамотности, основ безопасности информационных систем, поведению в сети Интернет.

Таким образом, организация борьбы с кибертерроризмом требует многогранного и комплексного подхода, осуществления совместных действий и принятия решений. Рост разнообразных вызовов и угроз кибертерроризма требует реализации комплексов основных технических мер для борьбы за безопасность при работе с информацией.

Именно соблюдение специальной системы мер по обеспечению надежности информационной безопасности поможет эффективно противостоять кибертеррористам, поскольку их способы схожи с инструментарием, применяемым киберпреступниками.

Заключение

1. Современное виртуальное пространство расценивается террористическими и экстремистскими организациями как новый вид инструмента для достижения своих целей. С его использованием террористов воспитывают не в подпольных лагерях и конспиративных квартирах, а проникая через компьютеры и смартфоны в их сознание.

2. Современные угрозы террористического характера в глобальной виртуальной сети подразделяют на несколько основных крупных направлений:

– распространение радикальной идеологии;

– вербовку (вовлечение) новых членов в террористические и экстремистские организации;

– планирование, согласование, организацию и синхронизацию актов терроризма.

Современные реалии свидетельствуют о том, что потенциальные угрозы террористического характера также могут быть связаны с целенаправленными попытками информационно-психологического воздействия на отдельные группы населения, а также при определенных условиях с прямым шантажом и ультиматумом в отношении отдельно взятого государства.

3. Нужно актуализировать необходимость противодействия финансированию терроризма с использованием Глобальной сети как платформы, которая позволяет осуществлять перевод и распределение денежных средств по всей ее структуре. Область противодействия при этом несколько шире за счет организации в этой же сети структур снабжения материально-техническими ресурсами (вплоть до аренды жилого и нежилого помещений, легкового и грузового автотранспорта и т. д.).

4. Учет существующих различных определений кибертерроризма и проведенный в

рамках исследования анализ его содержания обуславливают целесообразность разработки его авторского определения. Представляется, что кибертерроризм – целенаправленное деструктивное влияние определенных субъектов на пользователей виртуальной сети посредством использования информационно-телекоммуникационных средств, технологий, методов с целью повышения напряженности, стимулирования «панических атак»; создания угроз, причинения имущественного ущерба (вреда), наступления иных тяжких последствий как для отдельной категории лиц, так и для всего общества в целом, а также последующего воздействия на принятие необходимых решений в различных отраслях и сферах жизнедеятельности.

5. Противодействовать негативному контенту, способствующему вовлечению в деструктивную деятельность посредством использования массмедиа и информационно-телекоммуникационной сети, в том числе сети Интернет, следует комплексно, в первую очередь с учетом реализации трех основных направлений: организационно-правового, идеологического и технического.

Эффективность информационно-пропагандистских методик противодействия идеологии терроризма определяется не только деятельностью государственных структур, но и во многом зависит от повсеместного и полноправного вовлечения в этот процесс многочисленных институтов гражданского общества.

СПИСОК ИСТОЧНИКОВ

1. Ермолович В. Ф., Галезник М. В. Версии при расследовании преступлений : моногр. Минск : ИНБ Республики Беларусь, 2009. 215 с.

2. Ахъядов Э. С.-М. Государственная политика в сфере противодействия информационному терроризму // Право и государство: теория и практика. 2025. № 4. С. 469–471. http://doi.org/10.47643/1815-1337_2025_4_469.

3. Гущина А. А., Пакляченко М. Ю. К вопросу терроризации медиаконтента // Противодействие терроризму и экстремизму в информационных системах : сб. науч. статей Всерос. конф. М. : Московский университет МВД России имени В. Я. Кикотя, 2020. С. 103–105.

4. Овсяник А. И., Сергеенкова Н. А. Информационный терроризм в современных условиях // Безопасность в современном мире. 2024. № 4 (5). С. 61–69.

5. Асанова И. П., Душенков И. В. Информационный терроризм: актуальность и особенности // Кооперация науки и общества как инструмент модернизации инновационного развития : материалы Междунар. науч.-практ. конф. (Саранск, 23–24 апр. 2024 г.) Саранск : МГПУ, 2024. С. 264–268.

6. Смирнов А. А. Организация контрпропаганды в области борьбы с терроризмом и экстремизмом: науч.-практ. пособие / под ред. А. П. Новикова. М. : АТЦ СНГ, 2020. 232 с.

7. Терроризм как социально-политическое явление: противодействие в современных условиях : моногр. / Ю. И. Авдеев, В. Ю. Бельский, А. И. Костин [и др.] / под ред. В. Ю. Бельского, А. И. Сацуры. М. : ЮНИТИ-ДАНА, 2015. 367 с.

8. Булавкин А. А., Османов М. М., Рябко Н. В. К вопросу о профилактике радикальной идеологии терроризма и экстремизма в сети Интернет: теоретические аспекты и способы противодействия // Российский научный вестник. 2025. № 1. С. 200–205.

9. Клочкова Е. Н. Кибертерроризм как одна из форм проявления современного терроризма // Противодействие терроризму и экстремизму в информационных системах : сб. науч. статей Всерос. конф. (Москва, 17 дек. 2020 г.). М. : Московский университет МВД России имени В. Я. Кикотя, 2020. С. 100–102.

REFERENCES

1. Ermolovich V. F., Galeznik M. V. Versions in the investigation of crimes : monograph. Minsk : Institute of National Security of the Republic of Belarus, 2009. 215 p. (In Russ.)

2. Akhyadov E. S.-M. State policy in the field of countering information terrorism // Law and state: theory and practice. 2025. No. 4. P. 469–471. http://doi.org/10.47643/1815-1337_2025_4_469. (In Russ.)

3. Gushchina, A. A., Paklyachenko, M. Yu. On the issue of terrorizing media content // Counteracting terrorism and extremism in information systems: collection of scientific articles of the all-Russian conference. Moscow : Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. Kikot, 2020. P. 103–105. (In Russ.)

4. Ovsyanik A. I., Sergeenkova N. A. Information terrorism in modern conditions // Security in the modern world. 2024. No. 4 (5). P. 61–69. (In Russ.)

5. Asanova I. P., Dushenkov I. V. Information terrorism: relevance and features // Cooperation of science and society as a tool for modernizing innovative development : proceedings of the International scientific and practical conference (Saransk, April 23–24, 2024). Saransk : Mordovian State Pedagogical University, 2024. P. 264–268. (In Russ.)

6. Smirnov A. A. Organization of counter-propaganda in the field of combating terrorism and extremism : scientific and practical manual / ed. by A. P. Novikov. Moscow : CIS Anti-Terrorism Center, 2020. 232 p. (In Russ.)

7. Terrorism as a socio-political phenomenon: counteraction in modern conditions : monograph / Yu. I. Avdeev, V. Yu. Belsky, A. I. Kostin [et al.] ; ed. by V. Yu. Belsky, A. I. Satsura. Moscow : UNITI-DANA, 2015. 367 p. (In Russ.)

8. Bulavkin, A. A., Osmanov, M. M., Ryabko, N. V. On the issue of prevention of radical ideology of terrorism and extremism on the Internet: theoretical aspects and methods of counteraction // Russian scientific bulletin. 2025. No. 1. P. 200–205. (In Russ.)

9. Klochkova E. N. Cyberterrorism as one of the forms of manifestation of modern terrorism // Counteraction to terrorism and extremism in information systems : collection of scientific articles of the all-Russian conference (Moscow, December 17, 2020). Moscow : Moscow University of the Ministry of Internal Affairs of Russia named after V. Ya. Kikot, 2020. P. 100–102. (In Russ.)

Информация об авторах:
Бадамшин И. Д. – кандидат юридических наук, доцент;
Савич М. В. – кандидат юридических наук, доцент.

Information about the authors:
Badamshin I. D. – Candidate of Law, Associate Professor;
Savich M. V. – Candidate of Law, Associate Professor.

Статья поступила в редакцию 31.07.2025; одобрена после рецензирования 31.07.2025; принята к публикации 17.11.2025.

The article was submitted 31.07.2025; approved after reviewing 31.07.2025; accepted for publication 17.11.2025.