

Абрамян С. К. – доцент кафедры специальных дисциплин Краснодарского университета МВД России, кандидат юридических наук, доцент (Россия, г. Краснодар)

ПРОТИВОДЕЙСТВИЕ ИНФОРМАЦИОННОМУ ТЕРРОРИЗМУ В СОВРЕМЕННОЙ РОССИИ

COUNTERING INFORMATION TERRORISM IN MODERN RUSSIA

Аннотация. Статья посвящена исследованию феномена информационного терроризма в современном мире, характеризующегося активным влиянием на общественное сознание и подрывом социальной стабильности благодаря развитым технологиям и доступности интернета. Рассматриваются ключевые виды информационного терроризма, такие как дезинформация, пропаганда, кибертерроризм и социальные манипуляции, их характерные особенности и возможные последствия. Анализируются риски, возникающие вследствие распространения ложной информации, пропаганды, нарушений в функционировании критической инфраструктуры и информационных атак. Автор подчеркивает важность понимания природы информационного терроризма для разработки действенных мер по предупреждению и нейтрализации его последствий, включая образовательные инициативы и совершенствование нормативно-правовой базы.

Ключевые слова: информационный терроризм, дезинформация, пропаганда, кибертерроризм, социальные манипуляции, общественное сознание, информационная безопасность, политический экстремизм, международное сотрудничество.

Abstract. This article explores the phenomenon of information terrorism in the modern world, which is characterized by its active influence on public consciousness and its ability to undermine social stability due to advanced technologies and the availability of the internet. It examines the key types of information terrorism, such as disinformation, propaganda, cyberterrorism, and social manipulation, as well as their characteristics and potential consequences. The article analyzes the risks associated with the spread of false information, propaganda, disruptions in critical infrastructure, and information attacks. The author emphasizes the importance of understanding the nature of information terrorism in order to develop effective measures to prevent and neutralize its consequences, including educational initiatives and improvement of the legal framework.

Keywords: information terrorism, disinformation, propaganda, cyberterrorism, social manipulation, public consciousness, information security, political extremism, international cooperation.

Информационное пространство XXI века претерпело кардинальные изменения, став площадкой для интенсивного взаимодействия множества авторов: государств, коммерческих компаний, негосударственных организаций и индивидуальных участников. Одновременно оно превратилось в поле острых информационных баталий, где идет борьба за доминирующее положение в восприятии действительности и утверждение определенного видения мировых событий. Одной из серьезнейших угроз в новом веке стал информационный терроризм – активная эксплуатация коммуникативных каналов для оказания давления на общество, подрыва его устоев и дестабилизации ситуации. В условиях всепроникающего интернета любые силы могут оказывать мощное влияние на общественные настроения, ставить под сомнение легитимность власти, способствовать возникновению гражданских протестов и революций. Поэтому понимание сущности информационного терроризма и его возможных последствий становится актуальным вопросом безопасности как отдельного гражданина, так и целой страны.

Информационный терроризм трактуется как целенаправленное воздействие на индивидуумов и массы посредством манипулирования информацией с целью внесения изменений в поведение, установку определенных менталитетов, дестабилизации ситуаций или разрушения основ существующей социальной структуры. Чаще всего речь идет о целенаправленном применении информационных техник, обеспечивающих возможность добиваться поставленных целей с минимальным риском для организаторов и исполнителей операций.

История появления термина уходит корнями в XIX век, когда была отмечена взаимосвязь информационных технологий и использования специальных методик для достижения политических целей. Наиболее известным примером ранних этапов становления феномена были разведывательно-диверсионные операции, проводившиеся спецслужбами имперских держав Европы и России. Позже термин получил новое звучание в связи с появлением радио, телевидения и, наконец, интернета, расширивших арсенал воздействий и позволивших выйти на качественно новый уровень [1, с. 37].

Сегодня понятие охватывает не только классические приемы дезинформации и психологической войны, но и новые формы вроде целенаправленного размещения вбросов, манипулирования пользователями социальных сетей, разработки и распространения вирусов, атак на информационные системы.

Классификация видов информационного терроризма базируется на особенностях используемых методов и целях организаторов. Выделяются четыре основных категории:

1. Дезинформация. Ее смысл сводится к подаче ложных или частично искаженных сведений, что приводит к ошибочным выводам и принятию неправильных решений. Пример – публикации фейковых новостей, нацеленных на создание атмосферы паники или смятения.

2. Пропаганда. Включает методологию формирования устойчивых взглядов и установок. Может реализовываться открыто или завуалированно, применяя символику народов, культурные стереотипы и историческую память.

3. Кибертерроризм. Характеризуется действиями, направленными на нарушение функционирования компьютерной техники, ПО и прочих компонентов цифрового окружения. Распространенными приемами выступают хакерские вторжения, DDoS-нападения, похищение конфиденциальных данных, внедрение вредоносных программ.

4. Социальные манипуляции. Применяется для целенаправленного изменения мнения и поступков значительных социальных слоев. Типичные подходы заключаются в эксплуатации автоматизированных аккаунтов, создании поддельных онлайн-сервисов, организации массовых акций и демонстраций.

Все перечисленные разновидности представляют серьезную угрозу государству и социуму, поскольку затрагивают самые важные сферы человеческой жизнедеятельности: интеллектуальное восприятие реальности, поведенческие паттерны, техническую инфраструктуру.

Источники, инициирующие террористические акции в информационном пространстве, многообразны и разнятся по своим мотивам и основаниям. Среди них: группы радикально настроенных активистов, чьи цели связаны с изменением политической ситуации или достижением конкретной цели (например, ликвидация какого-либо лидера); корпорации, стремящиеся вытеснить конкурентов, добиться выгодных контрактов или повлиять на общественное мнение; спецслужбы иностранных государств, пытающиеся провести операцию по изменению международной обстановки или ослаблению противника; преступные группировки, извлекающие прибыль из шантажа, вымогательства и продажи незаконно полученных данных. Факторы мотивации террористов весьма разнообразны: от личного обогащения до удовлетворения амбициозных устремлений либо идеологических мотиваций.

Для достижения целей информационного терроризма применяется целый арсенал тактик и методов. Рассмотрим некоторые из них: троллинг и флэш-мобы. Используется для привлечения внимания к определенной проблеме, инициирования обсуждений и смены фокуса дискуссий. Методы маскировки и криптографии. Помогают скрыть следы пребывания в информационной среде, позволяя избегать преследования правоохранными орга-

нами. Создание дипфейков и фотошопов. Данные технологии помогают фабриковать убедительную картинку или видео, способные заставить поверить в реальность произошедшего. Метод «войн троллей». Осуществляется посредством автоматизации деятельности тысяч аккаунтов, пишущих одинаковые посты или реагирующих одинаково на конкретные запросы. Отдельно отметим высокую адаптивность террористических групп к изменениям в окружающей среде. Например, популярность социальных сетей привела к бурному развитию таргетированной рассылки фейковых сообщений, стриминга видеороликов и запугивания с помощью картинок или звукозаписей. Информационный терроризм угрожает каждому элементу государственной системы и затрагивает всех членов общества. Далее рассмотрим основные последствия его реализации. Одной из центральных целей информационного терроризма является подрыв доверия граждан к действующему правительству и администрации. Простота доступа к информации и возможность производить массивные объемы данных сделали его эффективным инструментом политического влияния. Операции, направленные на компрометацию высокопоставленных чиновников, внесение путаницы в законодательство или поддержку оппозиционеров, получили широкую известность. Еще одним следствием оказывается искаженное восприятие роли государства, которое утрачивает связь с народными чаяниями и ожиданиями, теряет способность своевременно реагировать на потребности общества.

Экономические эффекты информационного терроризма проявляются в следующем: ухудшается инвестиционный климат из-за подозрения инвесторов в ненадежности предприятий и рынка в целом; повышаются издержки, связанные с обеспечением кибербезопасности, уменьшением скорости оборота капитала и сокращением объема торговли; происходит снижение производительности труда и доходности компаний, пострадавших от информационных атак; экономика превращается в еще один объект приложения информационных ударов, результатом которого становится заторможенный экономический рост и увеличение бедности [2, с. 111].

Основными элементами социальных эффектов являются следующие аспекты: формирование тревожности и неопределенности среди населения, что приводит к понижению уровня удовлетворенности жизнью и качеству жизни; ослабление социальных связей, сопровождающее фрагментацию общества и уменьшение степени солидарности; увеличение уровня неравенства и социального дисбаланса, ускоряется деградация духовных ориентиров и культурных традиций. Информационный терроризм буквально разрушает социальные ткани общества, провоцирует рост радикальных настроений и потерю веры в традиционные институты власти. Противостоять информационному терроризму непросто, так как требуются совместные усилия государства, бизнеса и общества. Законодательство является ключевым элементом защиты от информационного терроризма. Ос-

новными мерами являются: принятие закона о запрете распространения ложной информации; установление уголовной ответственности за публикацию дезинформации и совершение преступлений с использованием цифровых технологий; организация надзорных органов, контролирующих исполнение законодательства в данной сфере. Также целесообразно вводить обязательные требования по маркировке новостей и комментированию в интернете, внедряя механизмы верификации учетных записей и отчетов об источниках финансирования кампаний.

Библиографический список

1. Манукян А. Р. Проблемы противодействия терроризму и экстремизму в сети Интернет в условиях повсеместной цифровизации // Пробелы в российском законодательстве. 2021. Т. 14, № 3. С. 37–41.

2. Сальников Е. В. Проблемы противодействия экстремизму: минимизация и (или) ликвидация его последствий в составе механизма противодействия экстремизму // Ленинградский юридический журнал. 2011. № 3 (25). С. 107–118.

© Абрамян С. К., 2026

УДК 342. 9

Алешин С. В. – доцент кафедры административно-правовых дисциплин Уфимского юридического института МВД России (Россия, г. Уфа)

К ВОПРОСУ ОХРАНЫ ОБЩЕСТВЕННОГО ПОРЯДКА И ОБЕСПЕЧЕНИЯ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

ON THE QUESTION OF PROTECTING PUBLIC ORDER AND ENSURING PUBLIC SAFETY

Аннотация. В статье изучаются понятия «общественный порядок», «общественная безопасность», рассматривается роль полиции в реализации данных государственных задач, анализируются правовые основы данной деятельности. Акцентируется внимание на необходимость взаимодействия всех государственных структур, общественных объединений, граждан в вопросах охраны общественного порядка и обеспечения общественной безопасности. Автором делается вывод о необходимости совершенствования системы общественной безопасности, требующей от государства комплексного подхода.