DOI 10.35775/PSI.2025.123.6.038
УДК 32

В.А. ДАНИЛОВ
кандидат исторических наук, доцент
кафедры теории и истории международных отношений,
директор центра прикладного анализа международных трансформаций
РУДН им. П. Лумумбы, Россия, г. Москва
E-mail: danilov_va@pfur.ru

Е.И. СОБОЛЕВ
студент кафедры теории и истории международных
отношений РУДН им. П. Лумумбы, Россия, г. Москва
E-mail: 1132231370@pfur.ru

М.А. ЗИНОВИН
аспирант направления «Международные отношения»
кафедры теории и истории международных отношений
РУДН им. П. Лумумбы, Россия, г. Москва
E-mail: zinovin_ma@pfur.ru

СОВРЕМЕННЫЕ IT-ТЕХНОЛОГИИ КАК ОДИН ИЗ ИНСТРУМЕНТОВ ТЕРРОРИЗМА В 21 ВЕКЕ

В статье рассматривается проблема использования современных информационных технологий (ИТ) террористическими организациями в XXI веке. Анализируются методы и способы применения ИТ в целях пропаганды, вербовки, координации действий и осуществления террористических актов. Особое внимание уделяется вопросам кибертерроризма, распространению экстремистской идеологии в сети Интернет и роли социальных сетей в радикализации населения. Предлагаются подходы к противодействию использованию ИТ в террористической деятельности.

Ключевые слова: *ИТ-технологии, терроризм, кибертерроризм, пропаганда, вербовка, экстремизм, информационная безопасность, противодействие.*

Терроризм представляет собой систему взглядов, оправдывающую насилие, и комплекс мер, направленных на оказание давления на государственные органы, органы местного самоуправления и международные структуры с целью принуждения к принятию определенных решений посредством запугивания населения и/или совершения иных противозаконных насильственных действий [27. П. 1, ст. 3].

Терроризм как глобальное явление выходит за рамки отдельных государств, а вопросы, касающиеся его распространения и финансовой подпитки, являются предметом обсуждения на высшем политическом уровне.

Следует подчеркнуть, что в работах российских и зарубежных авторов, опубликованных в последние годы, освещается широкий спектр вопросов близких к данной предметной области [1; 3; 4; 6; 7; 8; 9; 10; 13; 15; 16; 18; 19; 21; 26; 28].

Однако проблему противодействия использованию ИТ в террористической деятельности и искоренения терроризма нельзя назвать однозначно исчерпанной. В силу многих объективных обстоятельств изучение обозначенной темы продолжает сохранять высокий уровень актуальности.

Актуальность проблемы обусловлена растущей деятельностью международных и региональных террористических группировок. С учетом текущей геополитической обстановки, уровень террористической опасности существенно возрастает.

Вербовка через интернет носит глобальный характер, однако наиболее активные зоны включают регионы с высоким уровнем социально-экономической нестабильности и политической напряженности. Согласно данным Global Terrorism Index (2023), страны Ближнего Востока, Африки и Южной Азии остаются наиболее уязвимыми перед онлайн-вербовкой [31. С. 42]. Наиболее восприимчивой к вербовочным действиям террористических организаций являются молодые люди в возрасте от 15 до 30 лет.

В условиях становления современного информационного общества, транснациональные террористические группировки все активнее интегрируют передовые технологические решения в свою противоправную деятельность, что создает ощутимую угрозу национальной безопасности государств [11. С. 31]. Феномен международного терроризма следует интерпретировать в контексте глобальной политической конъюнктуры как предвестник эпохи «информационных войн».

Террористические организации эффективно используют информационную среду, включая средства массовой информации и Интернет, для распространения своей идеологии, пропаганды социальной, расовой, религиозной и национальной нетерпимости, а также для поиска и вербовки новых членов, имеющих образование, представляющее интерес для террористов [24. С. 8].

Террористические организации используют различные методы онлайн-вербовки, включая: прямую пропаганду, персонализированный подход, создание онлайн-сообществ, использование игровых платформ.

Организации, признанные террористическими, активно используют платформы, такие как Telegram, TikTok, VK, и др., для распространения пропагандистских материалов. Эти материалы часто содержат идеализированные образы террористов, то есть демонстрируются изображения и видео, представляющие участников противоправных ячеек как героев, борющихся за «правое дело». Эти образы часто контрастируют с реалиями конфликтов, представляя искаженную картину происходящего. Стоит также отметить прямые призывы к участию в вооруженной борьбе, часто основанные на религиозной риторике и направленные на радикализацию и мобилизацию потенциальных новобранцев. Кроме того, террористы прибегают к манипуляции новостными сюжетами, то есть

искажению фактов и распространению дезинформации с целью оправдания насилия и демонизации противников [5. С. 46].

Террористы создают контент, ориентированный на молодежь: они используют мемы, видеоигры и другие популярные форматы для привлечения внимания молодых пользователей и постепенной индоктринации. Так, например, ИГИЛ (запрещенная в России организация) активно использовала Twitter для распространения видеороликов с кадрами успешных операций и призывами к присоединению к «халифату». Эти ролики сопровождались хэштегами, позволяющими охватить широкую аудиторию, а количество аккаунтов, использованных террористами, составило 46 тысяч [29. С. 7].

Кроме того, через подобные каналы осуществляется планирование, подготовка и координация террористических актов, а также сбор средств для финансирования террористической деятельности. Важно отметить стремление террористических элементов к проведению кибертеррористических атак, направленных на критически важную информационную инфраструктуру. Основная цель террористов заключается в максимально широком распространении своей идеологии среди общественности, оказании психологического воздействия на реальных и потенциальных жертв, органы государственной власти и мировое сообщество, а также в расширении своих рядов за счет новых рекрутов [12. С. 11].

После блокировки аккаунтов в крупных социальных сетях, вербовщики перешли к использованию закрытых онлайн-сообществ и зашифрованных каналов связи, таких как Telegram, Signal и WhatsApp. Эти платформы обеспечивают более высокий уровень анонимности и позволяют избежать мониторинга со стороны правоохранительных органов.

Вербовщики анализируют онлайн-активность пользователей, выявляя лиц, проявляющих интерес к экстремистской идеологии, испытывающих чувство отчуждения или находящихся в трудной жизненной ситуации.

После выявления потенциального новобранца, вербовщик устанавливает с ним личный контакт, часто представляясь единомышленником или наставником. Вербовщик постепенно углубляет знания новобранца в экстремистской идеологии, используя тщательно отобранные материалы и оказывая психологическое воздействие [14. С. 71-72].

После завершения процесса индоктринации, вербовщик оказывает помощь в организации поездки в зону конфликта, предоставляя информацию о маршруте, документах и контактах.

Так, например, Al-Shabaab (запрещенная в России организация) использует Telegram для распространения пропаганды и вербовки новых членов. Вербовщики создают закрытые группы, в которых обсуждаются вопросы религии, политики и джихада. В этих группах вербовщики выявляют наиболее восприимчивых членов и устанавливают с ними личный контакт для дальнейшей обработки [30. С. 26, 28].

Эффективная борьба с онлайн-вербовкой требует комплексного подхода, включающего следующие компоненты:

• усиление мониторинга социальных сетей. Разработка и внедрение эффективных алгоритмов для выявления и удаления экстремистского контента;

• сотрудничество с платформами социальных сетей. Активное взаимодействие с компаниями, владеющими социальными сетями, для усиления мер по борьбе с онлайн-вербовкой;

• образовательные программы. Проведение образовательных программ для молодежи, направленных на повышение медиаграмотности и критического мышления;

• международное сотрудничество. Укрепление международного сотрудничества в области борьбы с терроризмом, включая обмен информацией и опытом в сфере противодействия онлайн-вербовке.

С развитием инновационных финансовых инструментов, потенциально обеспечивающих анонимность транзакций, наблюдается их незамедлительное проникновение в неформальный экономический сектор. Данная тенденция характерна и для криптовалют, популярность которых неуклонно растет в контексте криминальной деятельности, выступая либо в качестве средства совершения противоправных деяний, либо в качестве объекта преступных посягательств.

Криптовалюта, в силу своей децентрализованной и псевдоанонимной природы, представляют собой привлекательный инструмент для террористических организаций, стремящихся к диверсификации источников финансирования. Использование криптовалюты позволяет обходить традиционные финансовые институты и механизмы контроля, затрудняя отслеживание транзакций и идентификацию бенефициаров.

Росфинмониторинг России указал, что им неоднократно фиксировались факты финансирования терроризма с использованием криптовалют, среди которых особенно популярны Bitcoin, Ethereum и Monero [22. С. 197].

Террористические группы используют онлайн-платформы, социальные сети и зашифрованные мессенджеры для распространения призывов к пожертвованиям в криптовалюте. Они часто апеллируют к идеологической солидарности и обещают использование средств для поддержки «правого дела». Примером может служить кампания по сбору средств в Bitcoin, организованная сторонниками ИГИЛ (запрещенная в России террористическая организация) в 2015-2016 годах, целью которой было финансирование террористической деятельности в Сирии и Ираке [32. С. 12].

Криптовалюты используются для отмывания доходов, полученных от таких преступлений, как вымогательство, киберпреступность, торговля наркотиками и контрабанда. Преступные доходы конвертируются в криптовалюту, которая затем переводится через несколько кошельков и криптовалютных бирж, расположенных в юрисдикциях с менее строгими нормами регулирования. Это

значительно затрудняет отслеживание первоначального источника средств и установление связи между преступлением и финансированием терроризма.

Террористические организации используют криптовалютные биржи и обменники для конвертации криптовалюты в фиатные деньги или другие цифровые активы. Они могут создавать фиктивные аккаунты, использовать украденные удостоверения личности и прибегать к другим методам обхода процедур KYC (Know Your Customer) и AML (Anti-Money Laundering). Наличие криптовалютных бирж, расположенных в странах с недостаточным регулированием, создает дополнительные возможности для анонимного проведения транзакций [32. С. 6]. Сегодня, несмотря на усилия по ужесточению регулирования, многие криптовалютные биржи все еще остаются уязвимыми для использования в преступных целях.

Даркнет, представляющий собой скрытую часть Интернета, доступную только через специализированное программное обеспечение, является платформой для торговли незаконными товарами и услугами, включая наркотики, оружие и украденные данные. Террористические организации используют этот сегмент всемирной Сети для приобретения необходимых ресурсов и обмена информацией, а криптовалюты, особенно Monero, обеспечивают анонимность транзакций [32. С. 15].

Для эффективного противодействия использованию криптовалют в финансировании террористической деятельности, целесообразно рассмотреть следующие меры:

• усовершенствование действующих механизмов международного сотрудничества;

• гармонизация обмена информацией об угрозах и унификация требований к кибербезопасности для усиления защиты критически важных секторов экономики, таких как финансовый сектор;

• введение временных санкций или других мер воздействия в отношении государств, демонстрирующих недостаточную активность в борьбе с киберпреступностью;

• развитие углубленного международного сотрудничества в правовой сфере для борьбы с киберпреступностью, учитывая трансграничный характер большинства преступлений, связанных с криптовалютами, включая финансирование терроризма.

Принимая во внимание транснациональную природу большинства преступлений, совершаемых с использованием криптовалют, в том числе в целях финансирования терроризма, данное взаимодействие должно осуществляться на наднациональном уровне.

Таким образом, терроризм в эпоху цифровых технологий представляет собой многоаспектную и динамично развивающуюся угрозу, требующую комплексного подхода к противодействию.

В контексте глобальной политической нестабильности и расширения цифрового пространства, усиление мер по противодействию онлайн-вербовке, мониторингу и пресечению финансирования терроризма с использованием криптовалют становится приоритетной задачей. Необходимо совершенствование нормативно-правовой базы, разработка и внедрение передовых технологий мониторинга и анализа, а также укрепление международного сотрудничества в данной сфере.

Эффективная борьба с терроризмом в цифровой среде требует координации усилий международных и государственных организаций частного сектора и гражданского общества. Важным аспектом является повышение уровня медиаграмотности населения по всему миру, особенно молодежи, для формирования критического мышления и устойчивости к воздействию пропагандистских материалов. Только комплексный и системный подход позволит эффективно противостоять угрозе терроризма в современном информационном обществе.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. **Абдурагимов З.Е.** Мягкие политические технологии профилактики терроризма // Вопросы политологии. 2024. № 9.
2. **Абисова К.С.** Информационные технологии как фактор трансформации террористической деятельности // Вестник экономической безопасности. 2022. № 2.
3. **Акопян Г.А.** Современный терроризм: ключевые особенности развития и проблемы его искоренения // Вопросы национальных и федеративных отношений. 2024. № 4.
4. **Араев С.И., Титов М.К.** Украинский неонацизм как инструмент политических элит стран Запада в борьбе с Россией // Вопросы политологии. 2024. № 5.
5. **Арипшев А.М.** Экстремизм и терроризм в социальных сетях: проблемы обнаружения и противодействия // Журнал прикладных исследований. 2022. № 9.
6. **Венцель С.В.** Роль субъектов профилактического воздействия в системе противодействия распространению политического экстремизма в среде новых медиа // Вопросы политологии. 2024. № 1.
7. **Дзахова Л.Х., Кадзова Н.** Трансформация угроз национальной безопасности в условиях усиления деструктивных сообществ в российском сегменте сети Интернет // Вопросы национальных и федеративных отношений. 2025. № 1.
8. **Залысин И.Ю., Старцева С.Г.** Современный терроризм: специфика, динамика, тенденции // Евразийский Союз: вопросы международных отношений. 2024. № 5.
9. **Залысин И.Ю.** Терроризм в Сахеле: причины, особенности, перспективы // Вопросы политологии. 2025. № 1.

10. **Климова А.С.** Контртеррористическая стратегия «Contest» в комплексе мер Великобритании по борьбе с терроризмом в первой четверти XXI в. (Часть I) // Вопросы политологии. 2024. № 10.
11. **Кобец П.Н.** Опыт и проблемы противодействия международному терроризму на объектах атомной энергетики // Научный портал МВД России. 2019. № 2 (46).
12. **Кобец П.Н.** Информационное воздействие как один из современных методов терроризма и меры борьбы с ним // Вестник КРУ МВД России. 2022. № 1 (55).
13. **Комерцов В.В., Харламова С.В., Григорян Д.К.** К вопросу о киберпреступлениях в онлайн пространстве // Евразийский Союз: вопросы международных отношений. 2025. № 1.
14. **Костева Т.Ю.** Вовлечение лица в преступную деятельность террористического характера в информационно-телекоммуникационном пространстве: криминалистически значимые аспекты // Известия ТулГУ. Экономические и юридические науки. 2023. № 1.
15. **Кузина С.И., Сагирян И.Г.** Социально-политические детерминанты формирования личности террориста // Вопросы национальных и федеративных отношений. 2024. № 9.
16. **Лустин К.А.** Истоки и факторы проявления терроризма в России // Вопросы политологии. 2023. № 4.
17. **Люев Р.Х.** Технологии распространения идеологии экстремизма и терроризма в глобальном информационном пространстве // Образование и право. 2021. № 6.
18. **Медведев Н.П.** Национализм и этнополитический экстремизм // Евразийский Союз: вопросы международных отношений. 2025. № 1.
19. **Мелконянц Г.А.** Терроризм как угроза безопасности в условиях актуальной стадии глобализации // Вопросы политологии. 2024. № 10.
20. **Миронов А.И.** Роль криптовалют в совершении преступлений террористической и экстремисткой направленности в современных условиях // Baikal Research Journal. 2023. № 4.
21. **Морозов И.Л.** Терроризм и иные формы негосударственного политически мотивированного насилия – проблема демаркации по тактическим и идеологическим компонентам // Вопросы политологии. 2024. № 8.
22. **Мурадян С.В.** Перспективы использования криптовалют для целей финансирования терроризма и меры по предупреждению указанной тенденции // Закон и право. 2022. № 5.
23. **Олейникова Е.А.** Противодействие экстремизму в сети Интернет // Законность. 2016. № 5 (979).
24. **Опалев А.В.** Современные информационные технологии как инструмент деятельности экстремистских и террористических организаций // Вестник Московского университета МВД России. 2022. № 5.
25. **Пучков Д.В.** Кибертерроризм как новая угроза // Виктимология. 2021. № 4.

26. **Слизовский Д.Е., Медведев Н.П.** Рецензия на статью С.А. Ланцова «Этнический терроризм и этнополитические конфликты XIX-XX вв.: анализ социально-политических факторов» // Вопросы национальных и федеративных отношений. 2020. № 1.
27. Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» // Официальный портал Президента России // http://www.kremlin.ru/acts/bank/23522.
28. **Хугаева А.А.** Социальные детерминанты мотивации терроризма // Вопросы национальных и федеративных отношений. 2024. № 11.
29. **Berger J.M. & Morgan J.** ISIS Twitter census: A snapshot of the Islamic State's official support network // Brookings Institution // https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf.
30. Combating Terrorism Center at West Point // CTC Sentinel, January 2024 // https://ctc.westpoint.edu/wp-content/uploads/2024/01/CTC-SENTINEL-012024.pdf.
31. Global Terrorism Index 2023: Measuring the Impact of Terrorism // Institute for Economics & Peace. Sydney, March 2023 // http://visionofhumanity.org/resources.
32. Terrorist financing: The global threat and the U.S. response. Reiss Center for Law and Security, 2017 // https://www.lawandsecurity.org/wp-content/uploads/2017/05/CLSCNASReport-TerroristFinancing-Final.pdf.

V.A. DANILOV
Candidate of Historical Sciences, Associate Professor
of the Department of Theory and History of International Relations,
Director of the Center for Applied Analysis of International Transformations
RUDN University named after P. Lumumba, Moscow, Russia

E.I. SOBOLEV
Student, Department of Theory and History
of International Relations RUDN University named
after P. Lumumba, Moscow, Russia

M.A. ZINOVIN
Postgraduate Student in International Relations
of the Department of Theory and History of International Relations
RUDN University named after P. Lumumba,
Moscow, Russia

CONTEMPORARY IT TECHNOLOGIES AS ONE OF THE TOOLS OF TERRORISM IN THE 21ST CENTURY

The article examines the problem of the use of modern information technologies (IT) by terrorist organizations in the 21st century. The methods and means of using IT for propaganda, recruitment, coordination of actions and the implementation of terrorist acts are analyzed. Particular attention is paid to the issues of cyberterrorism, the spread of extremist ideology on the Internet, and the role of social networks in the radicalization of the population. Approaches to countering the use of IT in terrorist activities are proposed.

Key words: *IT technologies, terrorism, cyberterrorism, propaganda, recruitment, extremism, information security, counteraction.*