

УДК 343.98

Костева Т.Ю.¹

**ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ
«ИНТЕРНЕТ» В ЭКСТРЕМИСТСКОЙ И ТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ:
ИСТОРИЯ И СОВРЕМЕННОСТЬ**

Тулский государственный университет

Kosteva T.Y.

**THE USE OF THE INTERNET INFORMATION AND TELECOMMUNICATION
NETWORK IN EXTREMIST AND TERRORIST ACTIVITIES: HISTORY AND
MODERNITY**

Tula State University

Аннотация: В статье рассматриваются вопросы появления кибертерроризма, вреда какой он наносит социуму в настоящее время, а также почему именно интернет-ресурсы являются средством достижения преступниками их деструктивных целей и какие меры по противодействию данных мероприятий необходимо принимать на государственном уровне.

Ключевые слова: экстремизм, терроризм, Глобальная сеть «Интернет», информационные сети, право, криминалистика

Abstract: The article describes how cyberterrorism appeared and what harm it does to society at the present time, as well as why Internet resources are a means for criminals to achieve their destructive goals and what measures to counteract these measures should be taken at the state level.

Keywords: extremism, terrorism, Global network "Internet", information networks, law, criminology

Преступления экстремистской направленности и террористического характера всегда наносят колоссальный вред, как отдельным личностям, так и обществу, и государству, в целом дестабилизируют обстановку и приводят к многочисленным жертвам.

В соответствии со статистикой преступлений, опубликованной МВД России в январе-декабре 2022 года, на территории Российской Федерации было зарегистрировано 983 преступлений экстремистского и террористического характера [1], совершенных с использованием информационно-телекоммуникационных технологий или в сфере

¹ Костева Татьяна Юрьевна – ассистент кафедры Истории государства и права ФГБОУ ВО «Тулский государственный университет».

компьютерной информации. В том числе, связанной с:

- публичными призывами к осуществлению террористической деятельности, публичное оправданием терроризма или пропагандой терроризма (ст. 205.2 УК РФ) – 490 (+55,6 % по сравнению с 2021 годом);

- публичными призывами к осуществлению экстремистской деятельности (ст. 280 УК РФ) – 493 (+8,4 % по сравнению с 2021 годом).

Кибертерроризм появился в 1970-х годах. В 1983 году был арестован первый в истории «виртуальный преступник» - группа хакеров под названием «Банда 414» (США), которая взломала 60 компьютеров. С начала 1990-х годов проявления кибертерроризма фиксируют довольно часто [2].

В аспекте рассматриваемой проблематики обратим внимание на два примечательных факта. В конце 1990-х годов американский эксперт Уэйн Раш, специализирующийся на проблемах в области информационно-телекоммуникационных технологий, прогнозировал, что «в недалеком будущем радикальные группы полностью будут адаптированы к использованию в сети «Интернет», как инструмента коммуникации, вербовки, сбора денежных средств, стратегического позиционирования, связи с медиа» [3, с. 43].

Несколько позднее, профессор коммуникаций университета г. Хайфе (Израиль) Габриэль Вайман, который начал отслеживать и изучать террористические web-сайты еще с середины 1990-х годов, в научной работе «Террор в Интернете: новая арена битвы, новые вызовы», указывал уже на восемь типовых направлений, по которым террористы реализуют свои цели в сети «Интернет». А именно: проведение психологических войн; поиск информации; обучение; сбор денежных средств; пропаганда; вербовка; организация сетей; планирование и координация действий [4, с. 51]

Рассмотрим, как ученые-юристы определяют сущность экстремизма и его основные черты.

Г.И. Демин дает определение экстремизма, описывая его, как явление, которое представляет собой деятельность общественных и религиозных объединений, устойчивых социальных групп, отдельных индивидов, придерживающихся расовой, национальной, социально-политической идеологии, религиозной нетерпимости и вражды с использованием насилия или угрозы его применения для достижения противоправных целей [5, с. 9].

Т.А. Аристархова к одному из основных признаков экстремизма в современное время относит использование в преступной деятельности информационно-телекоммуникационных технологий для распространения экстремистской деятельности [6].

Д.С. Глухарев разделяет это мнение и подчеркивает, что экстремисты активно

внедряют различные психологические приемы воздействия на пользователей сети «Интернет»: создают и публикуют видеоролики заложников, распространяют фотографии и видео нападений на сотрудников правоохранительных органов и обычных граждан [7].

А.Х. Валеев полагает, что сеть «Интернет» - удобное поле для экстремистской деятельности, где можно распространять экстремистские материалы среди большого количества пользователей как через веб-страницы, так и через мессенджеры, блоги и форумы [8].

Стремительно быстрое развитие информационных и телекоммуникационных технологий на сегодняшний день привело к тому, что они интенсивно внедряются во все сферы жизнедеятельности человека. Глобальная сеть «Интернет», информационные сети позволяют обмениваться информацией в кратчайшие сроки. Функционирование и существование современного общества невозможно представить без обмена информацией в информационных-телекоммуникационных системах.

Привлекательность Интернета для экстремистских и террористических организации обусловлена следующим:

- достаточно простым доступом;
- большими охватами аудитории во всем мире;
- анонимностью общения;
- высокоскоростной передачей сообщения;
- применением традиционных средств массовой информации, которые используют ресурсы Интернета как источники тем для публикаций.

Проведенный автором статьи анализ зарубежных и отечественных исследований по проблемам информационного противодействия в Интернете [9, 10] позволяет выделить широкий круг следующих направлений деятельности экстремистских и террористических организаций в информационном пространстве:

- осуществление информационно-психологических атак на сообщество глобальной сети «Интернет»;
- пропаганда экстремистских идеологий для оправдания насилия и достижения своих целей;
- создание виртуальной преступной сети;
- планирование и координация деятельности участников по совершению террористических актов;
- сбор сведений об объектах планируемых актов;
- хакерские атаки на государственные сайты и международные интернет – ресурсы.

На данный момент сложилась целая система радикальных интернет-сайтов на разных языках. Целью данных Интернет-ресурсов является религиозно-идеологическая подготовка будущих участников террористических группировок. В основном это сайты на арабском языке, которые ориентированы на соответствующие географические зоны. [11, 119 с.].

Подготовленные террористами электронные материалы публикуются на электронных площадках террористического характера, затем посетители копируют информацию и распространяют ее далее – на другие сайты как экстремистской направленности, так и неэкстремистской направленности. Такой процесс позволяет оперативно распространять пропагандистские материалы.

В русскоязычном сегменте Интернета созданы как «джихадистские» сайты, так и сайты, созданные украинскими неонацистами, которые разжигают национальные конфликты, оказывают деструктивное воздействие на личность, искажают исторические факты, преподнося радикальные идеи неонацизма как единственно верные.

На данный момент идеологи террористических организаций в своей пропагандистской деятельности все чаще используют документальные видео, аудио- и видео- сообщения посредством таких менеджеров, как Skype, WhatsApp, Telegram, Instagram, ВКонтакте.

Интернет-контент террористического характера нацелен на четыре типа аудитории [12].

Первый тип – «противники», которых нужно запугать, заставить выполнять требования террористов.

Второй тип – «международная собственность», у которой необходимо сформировать мнение о деятельности террористических и антитеррористических организаций. Поскольку на данный момент общественное мнение – приоритет, то задачей любого терроракта является информационно-пропагандистская акция, призванная привлечь внимание общественности.

Третий тип – «сочувствующие». Основной задачей работы с ними является агитация, вербовка, подготовка новых активистов.

Четвертый тип – активные члены, с которыми с помощью Интернета осуществляется связь.

Сайты, способствующие распространению идеологии экстремизма и терроризма, условно можно разделить на четыре группы [12].

Первая группа – сайты, которые распространяют идеи экстремизма, терроризма, ксенофобии и сепаратизма. Они проповедуют радикальные исламистские взгляды.

Вторая группа – сайты, призывающие к террористическим действиям,

пропагандирующие межнациональную рознь и межконфессиональные конфликты.

Третья группа – информационные сайты, разжигающие ксенофобию на основе национальной или расовой принадлежности. Например, антисемитские сайты.

Четвертая группа – справочные сайты, косвенно призывающие к совершению террористических актов. Это сайты, содержащие справочную информацию: как изготовить взрывчатое вещество кустарным способом, на каких интернет-сайтах можно найти контакты лиц, которые помогут получить необходимые для изготовления взрывчатых устройств материалы.

Таким образом, можно сделать вывод о том, что число преступлений, носящих экстремистский или террористический характер неуклонно растет. В связи с этим, необходимы следующие меры, которые, по нашему мнению, могли бы противодействовать распространению экстремизма и терроризма в информационном пространстве:

- функционирование в системе правоохранительных органов специальных подразделений постоянного мониторинга интернет – пространства и принятие своевременных мер по пресечению пропаганды политического и религиозного экстремизма, планируемых террористических актов;

- обеспечение надлежащей профессиональной подготовки специалистов подразделений по борьбе с кибертерроризмом с привлечением ученых, психологов, священнослужителей, блогеров, программистов, а также должностных лиц органов государственной власти;

- объединение усилий общественных, некоммерческих, религиозных, научных Интернет – сообществ, направленных на противодействие идеологии терроризму и экстремизму.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2022 года // Официальный сайт МВД России [Электронный ресурс] // URL: <https://мвд.рф/reports/item/35396677/> (дата обращения 28.03.2023).

2. Соколов А.С., Поволотцкий А.Ю. Кибертерроризм в России и странах Центральной Азии // Российско-азиатский правовой журнал, 2020. № 2.

3. Rash W. Politic on the nets: Wiring the political process. New York: W.H. Freeman, 1997.

4. Weimann G. Terror on the Internet: The New Arena. Washington, DC: United States Institute of Peace Press, 2006.

5. Демин Г.И., Кибак Г.И. Экстремизм, его содержание и формы. Участие органов

внутренних дел в предупреждении и пресечении правонарушений экстремистской направленности. Лекция. М.: 2013. - С 9.

6. Аристархова Т.А. Основные черты и особенности молодежного экстремизма // Известия Тульского государственного университета. Тула, 2014. № 1-2.

7. Глухарев Д.С. Противодействие экстремизму в современном медиапространстве // Вестник Южного Уральского государственного университета. Челябинск, 2012. № 10.

8. Валеев А.Х. Борьба с проявлением экстремизма в сети Интернет // Бизнес в законе, 2011. № 6.

9. Мюрид Э. ИГИЛ. «Исламское государство» и Россия. Столкновение неизбежно? М.: Книжный мир, 2016.

10. Сундиев И.Ю. Введение в оперативно-розыскную деятельность: учебное пособие / И.Ю. Сундиев. - М.: ЮНИТИ: Закон и право, 2011. – 189 С.

11. Роль средств массовой информации и Интернета в предупреждении терроризма: материалы IV-й Всероссийской научно-практической конференции (том 2). –М: Рос. Гос. Унив. нефти и газа им. И.М. Губкина: ОАО «Нефть и бизнес», 2013. – 119 С.

12. Костихин А.А. Интернет как инструмент террористических и экстремистских организаций в психологической войне [Электронный ресурс]. – URL: <http://www.iimes.ru/?p=4737> (дата обращения 28.03.2023).

REFERENCES (transliteration)

1. Kratkaya karakteristika sostoyaniya prestupnosti v Rossijskoj Federacii za yanvar` – dekabr` 2022 goda // Oficial`ny`j sajt MVD Rossii [E`lektronny`j resurs] // URL: <https://mvd.rf/reports/item/35396677/> (data obrashheniya 28.03.2023).

2. Sokolov A.S., Povolotczkij A.Yu. Kiberterrorizm v Rossii i stranax Central`noj Azii // Rossijsko-aziatskij pravovoj zhurnal, 2020. № 2.

3. Rash W. Politic on the nets: Wiring the political process. New York: W.H. Freeman, 1997.

4. Weimann G. Terror on the Internet: The New Arena. Washington, DC: United States Institute of Peace Press, 2006.

5. Demin G.I., Kibak G.I. E`kstremizm, ego sodержanie i formy`. Uchastie organov vnutrennix del v preduprezhdenii i presechenii pravonarushenij e`kstremistskoj napravlennosti. Lekciya. M.: 2013. - S 9.

6. Aristarxova T.A. Osnovny`e cherty` i osobennosti molodezhnogo e`kstremizma // Izvestiya Tul`skogo gosudarstvennogo universiteta. Tula, 2014. № 1-2.

-
7. Gluxarev D.S. Protivodejstvie e`kstremizmu v sovremennom mediaprostranstve // Vestnik Yuzhnogo Ural`skogo gosudarstvennogo universiteta. Chelyabinsk, 2012. № 10.
 8. Valeev A.X. Bor`ba s proyavleniem e`kstremizma v seti Internet // Biznes v zakone, 2011. № 6.
 9. Myurid E`. IGIL. «Islamskoe gosudarstvo» i Rossiya. Stolknovenie neizbezhno? M.: Knizhny`j mir, 2016.
 10. Sundiev I.Yu. Vvedenie v operativno-rozy`sknuyu deyatel`nost`: uchebnoe posobie / I.Yu. Sundiev. - M.: YuNITI: Zakon i pravo, 2011. – 189 S.
 11. Rol` sredstv massovoj informacii i Interneta v preduprezhdenii terrorizma: materialy` IV-j Vserossijskoj nauchno-prakticheskoy konferencii (tom 2). –M: Ros. Gos. Univ. nefi i gaza im. I.M. Gubkina: OAO «Neft` i biznes», 2013. – 119 S.
 12. Kostixin A.A. Internet kak instrument terroristicheskix i e`kstremistskix organizacij v psixologicheskoy vojne [E`lektronny`j resurs]. – URL: <http://www.iimes.ru/?p=4737> (data obrashheniya 28.03.2023).

Рецензент: Давыдов В.О. доцент кафедры правосудия и правоохранительной деятельности ФГБОУ ВО «Тулский государственный университет», доктор юрид. наук