

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРОТИВОДЕЙСТВИИ МЕЖДУНАРОДНОМУ ТЕРРОРИЗМУ: ТЕОРИЯ И ПРАКТИКА

Аннотация. В этой статье будет проанализировано, как информационные технологии трансформируют традиционные подходы к международному праву, включая аспекты кибербезопасности, защиты данных и цифровых прав.

Ключевые слова: международное право, международный терроризм, кибертерроризм, передовые технологии, информационные технологии.

MAZUROVA NATALYA NIKOLAEVNA

Postgraduate student at the Department of International Law
Herzen State Pedagogical University

INFORMATION TECHNOLOGIES IN COUNTERING INTERNATIONAL TERRORISM: THEORY AND PRACTICE

Abstract. This article will analyze how information technology is transforming traditional approaches to international law, including aspects of cybersecurity, data protection and digital rights.

Key words: international law, international terrorism, cyber terrorism, advanced technologies, information technologies.

В настоящее время общепризнанных понятий международного терроризма, а также понятия передовых технологий нет. Каждому понятию присущи свои общие черты и признаки. В современных условиях функционирования передовых технологий на стыке радикальных научных разработок и их применения, меняются способы взаимодействия террористических организаций, координации их контактов, ведения преступной деятельности.

Что же следует понимать под передовыми технологиями? Их следует охарактеризовать как новейшие технологии, которые, с одной стороны, способствуют решению глобальных проблем, а также способствуют и нарастанию новых вызовов в сфере международного терроризма, связанных с появлением новых форм его проявления, например, кибертерроризма.

В перечень передовых технологий входят в первую очередь цифровые технологии, такие как Интернет вещей (IoT), блокчейн, метавселенная, искусственный интеллект (ИИ), включая генеративный ИИ (GenAI), большие данные и облачные вычисления. В современных условиях следует своевременно пресекать активного использования возможностей цифровых технологий террористическими организациями.

Физические технологии, такие как автономное вождение, 3D-печать и аппаратные инновации упрощают организацию террористических атак с возможностью избежать наказания за террористические преступления. Например, перехват управления воздушным судном, либо морским судном, либо поезда, что неизбежно может привести большому количеству человеческих жертв.

Зарубежные ученые М. М. Абдул-Раззак и Р. Н. Нури анализируют природу цифрового терроризма, его характеристики и методы¹. В исследованиях Х. А. Ахмеда², С. Р. Аль-Абеди³, С. Х. Аль-Фатлави⁴ отмечается, что международный терроризм в цифровой среде направлен на достижение незаконных целей, таких как поражение цифровой структуры страны, ее изоляцию от

¹ Abdul-Razzaq M. M., Nuri R. N. The role of international organizations in combating digital terrorism // The Message of Rights magazine. 2018. No. 10 (2). Pp. 46-70. (In Arabian).

² Ahmed H. A. Electronic terrorism and the role of the international community in confronting it // Research Journal of the College of Basic Education. 2019. No. 15 (4). Pp. 599-622. (In Arabian).

³ Al-Abedi S. R. The reality of terrorism and its repercussions on the Iraqi economy for the period 2003-2016 // Karbala University Journal. 2018. No. 16 (1). Pp. 63-71. (In Arabian).

⁴ Al-Fatlawi S. H. The crAl-Zaidanin H. M., Al-Qaryouti R. M. Terrorism and its economic effects on Jordan // The Jordanian Journal of Islamic Studies. 2018. No. 14 (4). Pp. 129-144. (In Arabian).

внешнего мира и контроль за экономическим развитием, особенно в чувствительных секторах, включая финансовый сектор, который в большей степени взаимодействует с электронными средствами.

Современная доктрина международного права уделяет проблеме новых форм терроризма недостаточное внимание.

Глобальная контртеррористическая стратегия Организации Объединенных Наций, применяет общий стратегический и оперативный подход к борьбе с новыми формами проявления терроризма (далее Стратегия), изложенная в резолюции и прилагаемом к ней Плане действий (A/RES/60/288), состоит из четырех компонентов, а именно:

1. Устранение условий, способствующих распространению терроризма.
2. Меры по предотвращению терроризма и борьбе с ним.
3. Меры по укреплению потенциала государств по предотвращению терроризма и борьбе с ним и укреплению роли системы Организации Объединенных Наций в этой области.
4. Меры по обеспечению всеобщего уважения прав человека и верховенства права в качестве фундаментальной основы для борьбы с терроризмом.

В Стратегии закреплены основные руководящие принципы международного сотрудничества в сфере борьбы с терроризмом.

Выработанные меры борьбы недостаточны для противодействия современным формам международного терроризма, например кибертерроризм, и требуется существенная дальнейшая работа для развития системы борьбы с терроризмом. Генеральная Ассамблея проводит обзор Стратегии раз в два года и это делает ее живым документом, в котором учитываются приоритеты государств-членов в области борьбы с терроризмом¹.

Угроза кибертерроризма. С использованием информационно-коммуникационных технологий (ИКТ) в террористических целях запрещено Резолюцией Генеральной Ассамблеи Интерпола от 22 сентября 2005 г. № 10².

Конвенцию о преступности в сфере компьютерной информации от 23 ноября 2001 г., далее Будапештская конвенция³, можно применять при регулировании вопросов противодействия кибертерроризму.

С 2017 года проводятся консультации Спецкомитета ООН по разработке универсальной конвенции, как альтернативы Будапештской конвенции Совета Европы о компьютерных преступлениях по борьбе с киберпреступностью.

В 2019 году Россия добилась принятия Генеральной Ассамблеей ООН резолюции 74/247 «Противодействие использованию информационно-коммуникационных технологий в преступных целях» от 20.01.2020 г. о создании Специального комитета для «разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях». Данный специальный межправительственный комитет объединяет экспертов открытого состава, представляющих все регионы, для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях.

Переговорный процесс пережил несколько кризисов, 9 февраля 2024 года состоялось голосование по проекту и проект был отклонен ввиду различия позиций государств. Разногласия вызвало то, что рядом государств основная роль в будущем поиске ИКТ-преступников возлагается на Международный уголовный суд (МУС) в качестве альтернативы конвенции ООН по противодействию использованию ИКТ в преступных целях.

В США 13 августа 2024 года специальный комитет ООН по разработке конвенции принял текст проекта, а Россия сыграла одну из ключевых ролей в создании ее проекта.

¹ Генеральная Ассамблея Организации Объединенных Наций приняла резолюцию (A/RES/68/276) о четвертом обзоре Контртеррористической стратегии Организации Объединенных Наций.

² Addressing Internet activities supporting terrorism: resolution of the ICPO-Interpol Gen. Assembly, Berlin, 19-22 Sept. 2005, № AG-2005-RES-10. URL: <http://www.interpol.int/content/download/5386/45196/version/4/file/agn74res10.pdf> (дата обращения: 10.11.2024).

³ Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.). URL: <https://base.garant.ru/4089723/> (дата обращения: 10.11.2024).

В век информационных передовых технологий и информационных войн (netwar), практически все террористические организации ведут свою деятельность в медиа — сетях, стараясь захватить умы молодых людей, учитывая доступность и популярность социальных сетей в молодежной среде.

Если в 1998 году террористические структуры поддерживали в развивающейся на тот момент «всемирной паутине» всего 12 сайтов, в 2005 году — 4800, а в настоящее время их около 10 тысяч.

В сети функционирует большое количество новостных агентств и сайтов, напрямую не аффилированных с террористическими организациями, но разделяющих их идеологию и оказывающих террористам поддержку в различных формах.

Социальные сети сегодня превратились в мощный инструмент манипуляции сознанием и поведением молодых людей, способный эффективно влиять на общественное мнение. Главным образом эксплуатируется страх, чтобы мифологизировать угрозу экстремизма в общественном сознании, особенно это относится к молодежи.

Систематическое насаждение в массовом сознании представления о наличии угрозы экстремизма превращает его в символ, захватывающий образ, создавая в обществе впечатление о всемогуществе террора.

Этому способствует специфика глобальной сети, которая обеспечивает такие преимущества, как простота доступа, независимость от географического расположения, неограниченная потенциальная аудитория, высокая скорость передачи информации, анонимность коммуникации; трудности в осуществлении контроля со стороны правоохранительных органов.

Для адекватного реагирования на новые вызовы и угрозы уже недостаточно работать только силами спецслужб, необходимо объединение усилий государственных и общественных структур, власти, гражданского общества. Нельзя допустить, чтобы социальные медиа выступали в качестве рупора или ретранслятора идей экстремизма и терроризма.

СПИСОК ЛИТЕРАТУРЫ

1. Abdul-Razzaq, M. M. The role of international organizations in combating digital terrorism / M. M. Abdul-Razzaq, R. N. Nuri // *The Message of Rights magazine*. — 2018. — No. 10 (2). — Pp. 46–70. (In Arabian).
2. Ahmed, H. A. Electronic terrorism and the role of the international community in confronting it / H. A. Ahmed // *Research Journal of the College of Basic Education*. — 2019. — No. 15 (4). — Pp. 599–622. (In Arabian).
3. Al-Abedi, S. R. The reality of terrorism and its repercussions on the Iraqi economy for the period 2003–2016 / S. R. Al-Abedi // *Karbala University Journal*. — 2018. — No. 16 (1). — Pp. 63–71. (In Arabian).
4. Al-Fatlawi, S. H. Terrorism and its economic effects on Jordan / S. H. Al-Fatlawi, H. M. Al-Zaidanin, R. M. Al-Qaryouti // *The Jordanian Journal of Islamic Studies*. — 2018. — No. 14 (4). — Pp. 129–144. (In Arabian).