Научная статья
https://doi.org/10.24412/2220-2404-2024-8-25
УДК 343.9

ОСОБЕННОСТИ КИБЕРТЕРРОРИЗМА НА СОВРЕМЕННОМ ЭТАПЕ

Хасанов Р.Д.
Краснодарский университет МВД России

Аннотация. *Автором рассматривается сущность преступности в сфере террористической деятельности, совершаемой с использованием сети «Интернет». Обращается внимание на значимость данной угрозы для безопасности и защищенности многих государств на современном этапе развития. Оценивается степень возможных негативных последствий от развития такой преступности. Рассматривая актуальные тенденции исследуемой преступности и принимая во внимание специфику деятельности правоохранительных органов и особенности международного сотрудничества, автор формулирует возможные способы противодействия кибертерроризму.*

Цель. Исследование содержания кибертерроризма, его отличительных черт на современном этапе развития, вызовов, стоящих перед государствами по противодействию этому явлению и формулирование возможных шагов по разрешению обозначенных проблем.

Методы. Для достижения поставленной цели использовался нормативный подход в совокупности с общенаучными методами, такими как анализ, синтез, индукция, дедукция, а также специальными методами — формально-логическим, формально-юридическим, методом системного анализа.

Результаты. Изучение особенностей современного кибертерроризма способствует повышению эффективности правоприменительной деятельности правоохранительных органов.

Выводы. В статье предлагается авторское видение сущности кибертерроризма, оценка угроз, вызванных данным негативным явлением, а также целесообразных способов противодействия ему.

Ключевые слова: *кибертерроризм, информационно-телекоммуникационные системы, легализация, международное сотрудничество, меры предупреждения.*

FEATURES OF CYBERTERRORISM AT THE PRESENT STAGE

Rakhimdjon D. Khasanov
Krasnodar University of the Ministry of Internal Affairs of Russia

Abstract. *The author examines the essence of crime in the sphere of terrorist activity committed using the Internet. Attention is drawn to the significance of this threat to the security and safety of many states at the present stage of development. The degree of possible negative consequences from the development of such crime is assessed. Considering the current trends of the crime under study and taking into account the specifics of the activities of law enforcement agencies and the peculiarities of international cooperation, the author formulates possible ways to counter cyberterrorism.*

Target. A study of the content of cyberterrorism, its distinctive features at the current stage of development, the challenges facing states in countering this phenomenon and the formulation of possible steps to resolve the identified problems.

Methods. To achieve this goal, a normative approach was used in conjunction with general scientific methods, such as analysis, synthesis, induction, deduction, as well as special methods - formal logical, formal legal, method of system analysis.

Results. Studying the characteristics of modern cyberterrorism helps to increase the effectiveness of law enforcement activities of law enforcement agencies.

Conclusions. The article offers the author's vision of the essence of cyberterrorism, an assessment of the threats caused by this negative phenomenon, as well as appropriate ways to counter it.

Key words: *cyberterrorism, information and telecommunication systems, legalization, international cooperation, preventive measures.*

Введение.

Совершение преступных посягательств террористической направленности представляет серьезную угрозу для общественного порядка и общественной безопасности нашего государства. Данная проблематика также волнует и правоохранительные органы зарубежных стран, которые вынуждены учитывать специфику указанных преступлений в своей профессиональной деятельности.

В настоящее время, всеобъемлющая цифровизация и активное использование сети «Интернет» оказывают колоссальное влияние на появление новых форм и способов преступного поведения злоумышленников. Данная тенденция также затронула и противоправные деяния террористической направленности, что обуславливает актуальность избранной темы настоящей статьи. Преследуя основную цель в виде устрашения населения и оказания влияния на принятие органами власти значимых решений, злоумышленниками используется такое явление как «кибертерроризм».

Происходящая глобализация, в условиях которой осуществляется массовая миграция населения, изменяется национальный состав проживающих в странах лиц, также используется террористами для информационных атак по разжиганию ненависти между гражданами, которым предоставляется ложная информация о совершаемых аморальных и противоправных деяниях, бездействии органов власти, что требует самостоятельного решения таких надуманных проблем насильственным способом.

В свою очередь, государства должны изменять свою информационную политику, передавать населению сведения о современных способах действий террористов, налаживать международное сотрудничество, чтобы не допустить абсолютного роста данной преступности [1, с. 38].

По мнению И.В. Пащенко, начиная с 2000-х годов начинается активное использование террористическими организациями социальных сетей в целях максимального охвата аудитории на предмет их вовлечения в террористическую деятельность [2, с. 14].

Подчеркнем, что в 2023 г. в Российской Федерации было совершено на 29,7% больше преступлений с использованием информационно-телекоммуникационных технологий чем за 2022 г. Кроме того, возросло и количество преступных деяний в сфере терроризма на 6,7%, относительно аналогичного показателя 2022 г., что подтверждает важность углубленного рассмотрения избранной темы. Ярким примером такого противоправного действия в уголовном законодательстве России выступают публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (ст. 205.2 УК РФ). Аналогичные по содержанию преступления могут быть обнаружены в уголовном законодательстве зарубежных стран.

Результаты. В юридической периодике отсутствует единое видение сущности и содержания такого деструктивного явления как терроризм. Данное обстоятельство, безусловно, осложняет формулирование такого определения как кибертерроризм, под которым целесообразно понимать следующее:

1. Совершение террористических актов с использованием сети «Интернет», т.е. когда информационно-телекоммуникационная сеть выступает как способ и средство преступления.

2. Деятельность, которая способствует терроризму для вербовки новых участников, взаимодействия между имеющимися членами [3, с. 608].

При этом некоторые исследователи при осмыслении искомого понятия делают акцент именно на нанесении ущерба компьютерным данным и компьютерной информации в результате кибертеррористической атаки, что, как мы считаем, является лишь факультативными последствиями [4, с. 80]. Стоит при этом добавить, что в результате кибертерроризма, можно причинить вред информационной системе управления объектами инфраструктуры (транспорт, энергетика и т.д.), что может вызвать наступление тяжких последствий, например, сбой в работе атомной электростанции [5, с. 32].

Поскольку кибертерроризм немыслим без использования сети «Интернет», то и его отличительные черты также неразрывно связаны с особенностями информационно-телекоммуникационных систем:

- облегчение процесса обмена данными в разных точках земного шара, что исключает возможность встречи между лицами и усложняет процесс их идентификации и задержания. К примеру, через социальные сети осуществляется приискание новых членов террористического сообщества, далее им передается инструкция о совершении террористической акции, сообщается о местонахождении тайника с огнестрельным оружием, боеприпасами, иными поражающими элементами либо они осведомляются о том, как

можно самостоятельно изготовить взрывное устройство и привести его в действие;

- оказание воздействия в целях устрашения на неопределенное количество лиц в результате размещение видеозаписей, фотоматериалов о совершаемых и планируемых террористических атаках, что может вызывать панику и страх среди людей, а их опровержение правоохранительными органами не всегда доверительно воспринимается населением, что приводит к нарастанию напряжения в государстве;

- усиление большей зависимости государств в борьбе с этим явлением в виду того, что многие участники террористических организаций территориально находятся в разных странах, которые могут не взаимодействовать между собой, находиться в состоянии противостояния, что не позволит сосредоточить общие усилия на задержании и ликвидации преступников;

- использование быстрых систем платежей, в т.ч. электронной валюты, анонимных криптокошельков, что упрощает возможность передачи необходимых средств всем участникам террористического сообщества, затрудняет возможно выявления ресурсов правоохранительными органами, их ареста и изъятия;

- сбор информации о возможных объектах террористической атаки, поскольку многие планы внутреннего разграничения объекта, степени его защищенности, расположении входов и выходов из него могут быть размещены в сети «Интернет».

Необходимо описать алгоритм происходящей вербовки будущих террористов через сеть «Интернет». Он включает в себя следующие элементы:

- нахождение контакта (подбираются лица со сложными жизненными ситуациями, испытывающие психологический дискомфорт, ярые приверженцы справедливости, религиозные фанатики и проч.);

- возникновение мотивации (появление у человека чувства значимости в этом деле, давление на него в целях разрыва общения с родственниками и друзьями, демонстрация ему различного контента в целях формирования нужного мировоззрения);

- налаживание коммуникации (постоянное поддержание общения, привитие чувства нужности для общего дела, использование голосовых и видеосообщений);

- вступление в ряды террористической организации (предоставляется инструкция о действиях человека, куда и когда ему нужно прибыть для обучения либо выполнения террористической акции, ему передаются необходимые денежные средства, документы, оружие, иная значимая информация).

Заключение.

Полагаем, что современные особенности кибертерроризма ставят перед государствами множество задач, решение которых будет напрямую влиять на степень защищенности человека и гражданина в обществе:

- необходимость принятия единого международного правового акта, которым регламентировался бы порядок взаимодействия правоохранительных органов в сфере противодействия терроризму в сети «Интернет» (что могло бы быть освещено в рамках работы Организации Объединенных Наций);

- проведение постоянной модернизации нормативно-правовой базы по противодействию данному явлению (в частности, конкретизация законопроекта о конкретных правах, свободах и обязанностях человека в сети «Интернет», необходимой регистрации под персональными данными);

- создание более тесных связей при взаимодействии органов на различных уровнях по мониторингу информационно-телекоммуникационного пространства и ликвидации сведений, деструктивно-влияющих на население. Целесообразно усиление ответственности юридических лиц, которые своевременно не удалили и изъяли террористический контент [6, с. 62] (передача новейшего технического оборудования, позволяющего отслеживать такую информацию, эффективно и своевременно блокировать враждебные сайты);

- активизация противодействия финансированию терроризма, включая получение сведений из банковских организаций, препятствие обороту незаконно полученных электронных денежных средств и криптовалюты. Также, возможно использование общенационального электронного барьера, который фильтрует и контролирует информационные потоки, что используется в Китайской Народной Республике (наложение ареста и изъятия всего имущества, добытого преступного путем, в т.ч. предполагаемого для оплаты деятельности кибертеррористов);

- своевременное освещение среди населения сведений о новых угрозах террористической направленности, избираемых злоумышленниками способах вербовки членов террористических организаций, манипуляции мнением людей;

- вовлечение интернет-пользователей в процесс борьбы с противоправным контентом (в

особенности необходимо уделить внимание несовершеннолетним, которые могут стать легкой жертвой для террористов) [7, с. 38].

Таким образом, нами были отмечены особенности современного кибертерроризма, обращено внимание на сущности данного явления, а также те проблемы, которые требуют своего разрешения для эффективной работы правоохранительных органов.

Очевидно, что самым главным вызовом выступает соблюдение органами государственной власти баланса между обязанностью по защите и охране человека и гражданина от преступных посягательств и основополагающих прав и свобод людей относительно ограничения свободы слова, получения информации о частной жизни и иных фундаментальных гарантий.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование в формате double-blind peer review (рецензенту неизвестны имя и должность автора, автору неизвестны имя и должность рецензента). Рецензия может быть предоставлена заинтересованным лицам по запросу.

Conflict of Interest

None declared.

Review

All articles are reviewed in the double-blind peer review format (the reviewer does not know the name and position of the author, the author does not know the name and position of the reviewer). The review can be provided to interested persons upon request.

Литература:

1. Самохина Н.Н., Гутова С.Г. Феномен идеологии экстремизма и терроризма в сети Интернет: проблемы и пути их решения // Общество: политика, экономика, право. 2016. № 10. С. 37-41.

2. Пащенко И.В. Идеология террористических сообществ в сети Интернет: технологии распространения и специфика противодействия // Caucasian Science Bridge. 2018. № 1 С. 12-24.

3. Дремлюга Р.И., Коробеев А.И., Федоров А.В. Кибертерроризм в Китае: уголовно-правовые и криминологические аспекты // Всероссийский криминологический журнал. 2017. № 3. С. 607-614.

4. Мороз Н.О. Международно-правовая квалификация кибертерроризма // Вестник Марийского государственного университета. Серия «Исторические науки. Юридические науки». 2016. № 2. С. 79-84.

5. Капитонова Е.А. Особенности кибертерроризма как новой разновидности террористического акта // Известия высших учебных заведений. Поволжский регион. Общественные науки. 2015. № 2. С. 29-41.

6. Романовский Г.Б. Уголовная ответственность за акты терроризма во Франции // Наука. Общество. Государство. 2017. № 3. С. 58-64.

7. Лашин Р.Л., Чурилов С.А. Противодействие экстремизму и терроризму в сети Интернет и образовательной среде // Обзор. НЦПТИ. 2016. № 7. С. 34-39.

References:

1. Samokhina N.N., Gutova S.G. Phenomenon of the ideology of extremism and terrorism on the Internet: problems and solutions // Society: politics, economics, law. 2016. No. 10. Pp. 37-41.

2. Pashchenko I.V. Ideology of terrorist communities on the Internet: distribution technologies and specifics of counteraction // Caucasian Science Bridge. 2018. No. 1 Pp. 12-24.

3. Dremlyuga R.I., Korobeev A.I., Fedorov A.V. Cyberterrorism in China: criminal-legal and criminological aspects // All-Russian Criminological Journal. 2017. No. 3. Pp. 607-614.

4. Moroz N.O. International legal qualification of cyberterrorism // Bulletin of the Mari State University. Series "Historical Sciences. Legal Sciences". 2016. No. 2. Pp. 79-84.

5. Kapitonova E.A. Features of cyberterrorism as a new type of terrorist act // News of higher educational institutions. Volga region. Social sciences. 2015. No. 2. Pp. 29-41.

6. Romanovsky G.B. Criminal liability for acts of terrorism in France // Science. Society. State. 2017. No. 3. Pp. 58-64.

7. Lashin R.L., Churilov S.A. Counteracting extremism and terrorism on the Internet and in the educational environment // Review. NTsPTI. 2016. No. 7. Pp. 34-39.

Информация об авторе:

Хасанов Рахимджон Давлатович, адъюнкт очной формы обучения кафедры уголовного права и криминологии Краснодарского университета МВД России, https://orcid.org/0000-0002-5655-3750, e-mail: rahimjan.hasanov@bk.ru

Rakhimjon D. Khasanov, full-time adjunct student of the Department of Criminal Law and Criminology of the Krasnodar University of the Ministry of Internal Affairs of Russia.