Academic Research in Educational Sciences
ISSN: 2181-1385
DOI: 10.24412/2181-1385-2022-3-217-224

Volume 3 | Issue 3 | 2022
Cite-Factor: 0,89 | SIS: 1,12
SJIF: 5,7 | UIF: 6,1

НОРМАТИВНО-ПРАВОВАЯ БАЗА ЗАРУБЕЖНЫХ СТРАН И МЕЖДУНАРОДНЫХ ОРГАНИЗАЦИЙ В ОБЛАСТИ ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ

Азамат Кидирали угли Наркулов
Ведущий научный сотрудник Центра научно-прикладных исследований Университета общественной безопасности Республики Узбекистан

АННОТАЦИЯ

В статье рассматривается нормативно-правовая база зарубежных стран и международных организаций в области противодействия кибертерроризму, а также актуальные проблемы обеспечения международной и национальной кибербезопасности.

Ключевые слова: кибертерроризм, киберпространство, информационная безопасность, киберпреступность.

ВВЕДЕНИЕ

На сегодняшний день вопросы обеспечения информационной безопасности приобретают особую актуальность. Это обусловлено прежде всего происходящей масштабной цифровизацией важных отраслей экономики, систем государственного управления и общественного жизнеобеспечения. Наряду с преимуществами стремительного развития цифровых технологий, их проникновения во все сферы жизнедеятельности, возрастают риски неправомерного использования новых информационно-коммуникационных технологий для причинения ущерба объектам критической инфраструктуры.

В связи с этим возрастает необходимость развития многостороннего сотрудничества по вопросам реагирования на современные угрозы и инциденты кибербезопасности, расследования инцидентов и идентификации злоумышленников.

Угрозы кибертерроризма носят общерегиональный характер и, соответственно, требуют выработки общих подходов. Важным и эффективным средством является углубление взаимодействия между профильными ведомствами и органами в борьбе с экстремизмом не только в полевых условиях, но и в онлайн-пространстве.

Также немаловажную роль в данном вопросе играет уровень цифровой грамотности населения. Сегодня важно

реализовать совместные проекты по повышению уровня медиаграмотности граждан. Это позволит сформировать осознанное и ответственное потребление информации.

Растущая угроза кибертерроризма побудила государства и международные организации реформировать глобальную архитектуру кибербезопасности для борьбы с кибертерроризмом.

МЕТОДОЛОГИЯ

В нашей статье рассмотрим нормативно-правовые базы зарубежных стран и международных организаций.

Конвенция о киберпреступности

Конвенция Европейского Союза о киберпреступности, также называемая Будапештской конвенцией, является единственной обязательной международной конвенцией о киберпреступлениях. Она направлена на гармонизацию внутреннего законодательства, включая рамки международного сотрудничества, а также предлагает импровизировать методы расследования киберпреступлений для государств-членов.

Глобальная контртеррористическая стратегия ООН

Стратегия демонстрирует приверженность всех государств-членов ООН ликвидации терроризма во всех его формах. Резолюция направлена на расширение международного и регионального сотрудничества и координации между государствами, частными игроками и другими сторонами в борьбе с кибертерроризмом, а также направлена на противодействие распространению терроризма через киберсети. Резолюция 2018 года по шестому обзору стратегии призывает государства-члены обеспечить, чтобы киберпространство «не было безопасным убежищем для террористов». Он призывает государства-члены противодействовать пропаганде, подстрекательству и вербовке террористов, в том числе через киберпространство.

Контртеррористическое управление Организации Объединенных Наций (КТООН)

Контртеррористическое управление Организации Объединенных Наций было создано 15 июня 2017 года в соответствии с резолюцией Генеральной Ассамблеи Организации Объединенных Наций (ГА ООН) после доклада Генерального секретаря о роли ООН в оказании помощи государствам-членам в реализации стратегии ООН по борьбе с терроризмом. UNOCT дополняет усилия государств-членов

по борьбе с терроризмом, включая кибертерроризм. Он обеспечивает многостороннее сотрудничество в защите киберпространства соответствующих стран от кибертеррористических атак. Он инициировал различные проекты, направленные на создание и повышение потенциала государств для борьбы с кибератаками и повышение осведомленности масс о кибертерроризме.

Совет Безопасности ООН (СБ ООН)

В 2017 году СБ ООН принял резолюцию о защите КИ. В резолюции содержится призыв к государствам-членам наладить сотрудничество со всеми заинтересованными сторонами на международном и региональном уровнях для предотвращения, защиты, реагирования и восстановления после террористических атак с использованием кибернетики в отношении государственного КРУ. Он также просит штаты делиться оперативными данными об использовании коммуникационных технологий террористическими группировками. В заявлении Председателя СБ ООН в мае 2016 г. признается необходимость глобальных усилий, направленных на предотвращение использования киберсетей террористическими группировками.

Контртеррористическая стратегия Бразилии, России, Индии, Китая и Южной Африки (БРИКС)

Стратегия направлена на противодействие международному терроризму и его финансированию, расширение сотрудничества во взаимной правовой помощи и экстрадиции против террористов, улучшение практического сотрудничества между органами безопасности путем обмена разведданными и т.д. Стратегия направлена на «противодействие экстремистским нарративам, способствующим терроризму, и неправомерному использованию Интернет и социальные сети в целях вербовки, радикализации и подстрекательства к террористам, а также оказания финансовой и материальной поддержки террористам».

Шанхайская организация сотрудничества (ШОС)

ШОС предприняла несколько важных шагов для противодействия угрозе кибертерроризма. В 2001 году была создана Региональная антитеррористическая структура (РАТС) для борьбы с терроризмом. На 22-м заседании Совета РАТС ШОС были одобрены различные предложения по борьбе с кибертерроризмом, а также обсуждено предложение о создании Центра кибертерроризма. В 2019 году государства-члены ШОС провели учения по борьбе с кибертерроризмом, чтобы подготовиться к будущему кибертеррористическому

кризису. Кроме того, в 2015 году ШОС представила Генеральной Ассамблее ООН Международный кодекс поведения в области информационной безопасности, в котором предлагается безопасный и основанный на правилах порядок в киберпространстве. Кодекс предлагает международное сотрудничество между государствами для борьбы с использованием ИКТ в террористических операциях. Кроме того, он определяет кодекс поведения, обязанности государств и права отдельных лиц в киберпространстве.

Закон об Агентстве кибербезопасности и безопасности инфраструктуры (CISA)

Закон устанавливает, что CISA будет обеспечивать безопасность американских киберсетей и CI, разрабатывать структуры кибербезопасности США и развивать потенциал для защиты от кибератак. Кроме того, он защищает доменную сеть федерального правительства .gov. В нем также находится Национальный центр управления рисками (NRMC), который занимается большинством стратегических угроз для CI страны и критическими функциями, нарушение которых может иметь разрушительные последствия для национальных интересов США, таких как безопасность и экономика. В 2017 году президент США издал указ (EO 13800) о модернизации навыков кибербезопасности США в целях предотвращения усиливающихся угроз кибербезопасности в отношении КВОИ и других стратегических активов.

Национальная киберстратегия США

Стратегия, выпущенная в 2018 году, укрепляет киберпространство США для реагирования на кибератаки. Основное внимание уделяется обеспечению безопасности федеральных сетей и CI, а также борьбе с кибератаками. Киберстратегия в первую очередь направлена на защиту американского народа, сохранение мира и продвижение американских интересов. Он также предусматривает военные действия для борьбы с кибератаками.

Израиль

В 2017 году Израиль запустил свою первую в истории Национальную стратегию кибербезопасности. В политическом документе излагается план страны по повышению кибернадежности, системной устойчивости и гражданской национальной киберзащиты. Цель состоит в том, чтобы развивать международное сотрудничество в борьбе с глобальными киберугрозами, которые, безусловно,

включают угрозы кибертерроризма. Он также уделяет первоочередное внимание защите экономических, деловых и социальных интересов Израиля в киберпространстве.

Правительство Израиля приняло несколько резолюций, таких как 3611, 102, 2443 и 2444, для расширения институциональных возможностей системы кибербезопасности путем создания Национального киберуправления. Система кибербезопасности Израиля сосредоточена на четырех приоритетных областях:

Улучшение внутреннего потенциала для противостояния будущим и современным вызовам кибербезопасности.

Непрерывная модернизация и усиление защиты КВО в стране.

Повышение статуса республики как международного развития ИКТ.

Содействие эффективной координации и сотрудничеству между правительством, академическими кругами и частными игроками.

Соединенное Королевство (Великобритания)

В 2015 году Великобритания представила Национальную программу кибербезопасности для защиты своих компьютерных сетей от кибератак. В 2016 г. также была обнародована пятилетняя Национальная стратегия кибербезопасности, призванная сделать киберпространство Великобритании устойчивым к кибератакам и сделать его более безопасным к 2021 г. Кроме того, в 2017 г. был открыт Национальный центр кибербезопасности для реагирования на высококлассные кибератаки.

Закон о терроризме 2000 г. является законодательным актом Великобритании, вводящим в действие положения о терроризме, включая кибертерроризм. Раздел 1 Закона перечисляет три требования, чтобы квалифицировать акт как терроризм: намерение, мотив и вред. Закон предусматривает, что совершаемое действие должно иметь намерение оказать влияние на правительство или международную правительственную организацию либо запугать общественность или ее часть. Кроме того, акт должен быть направлен на продвижение политического, религиозного, радикального или идеологического дела. В Разделе 1(2) далее перечислены альтернативные виды вреда, которые могут быть причинены деянием, чтобы квалифицировать его как террористический акт. Он охватывает террористические акты, которые серьезно вмешиваются в работу электронной системы или нарушают ее работу. Термин «электронная система» может включать поставщиков интернет-услуг, поставщиков компьютеров, финансовых бирж и т. д.

Таким образом, закон Великобритании дает широкое определение терроризма. Сюда входят случаи кибератак на второстепенную инфраструктуру. Его можно применять к угрозе кибератаки так же, как и к фактической кибератаке. Он даже рассматривает случаи кибератак, направленных просто на «влияние» на правительство, как кибертерроризм, тем самым устраняя требование высших намерений, таких как принуждение или запугивание правительства.

Австралия

Австралия приняла законы о борьбе с терроризмом после теракта 11 сентября в виде группы из пяти законов. Закон о внесении поправок в законодательство о безопасности (терроризм) 2002 г. включил определение терроризма в часть 5.3 Уголовного кодекса Австралии. Статья 100.1 Уголовного кодекса дает определение терроризму. Австралийское законодательство устанавливает более высокие стандарты для акта, который может быть истолкован как терроризм, чем британский закон о терроризме. Таким образом, кибератаки с целью повлиять только на правительство не являются кибертерроризмом в Австралии. Согласно австралийскому законодательству, для признания кибертерроризм лицо своим действием должно иметь намерение принудить правительство или повлиять на него путем запугивания. Таким образом, кибератака должна быть принудительной или запугивающей. Применение австралийского закона о терроризме в случаях кибератак ограничивается только атаками, представляющими собой серьезное вмешательство, нарушение или уничтожение электронных систем. Закон также включает «исключение для политических протестов». Он устанавливает, что любая форма протеста, инакомыслия или иного не будет считаться терроризмом, если она не направлена на причинение смерти, серьезного физического вреда или угрозы жизни и т. д. Таким образом, в отличие от английского аналога, Уголовный кодекс Австралии признает более узкий круг кибератак как кибертерроризм.

Канада

Раздел 83.01 Уголовного кодекса Канады определяет терроризм как действие или бездействие, совершенное в Канаде или за ее пределами с политической, религиозной или идеологической целью, чтобы запугать общественность или часть людей, причинить серьезные телесные повреждения, смерть, создать угрозу жизни человека и т.д. Кроме того, канадский закон также

предусматривает исключение для политических протестов, как в Австралии. Однако он устанавливает очень высокие стандарты для акта терроризма, поскольку предусматривает, что такие акты должны «вынуждать» правительство действовать или воздерживаться от действий определенным образом. Сфера терроризма в канадском законодательстве распространяется на нападения на национальные и международные организации. Это устанавливает более широкую зону действия против «международных правительственных организаций», как в британском законодательстве. Канадское законодательство также квалифицирует нападение на человека как террористический акт. Кроме того, в нем предусматривается, что для того, чтобы представлять собой кибертерроризм, действие должно иметь намерение и вызвать фактическое вмешательство в основную систему, службу или объект. Это устанавливает еще один высокий стандарт в законе, позволяющий ввести в действие определение терроризма в случае кибератаки.

ВЫВОДЫ

Таким образом, разные страны дают разные определения акта кибертерроризма. Это разнообразие законов о терроризме препятствует глобальному сотрудничеству, поскольку эти различные определения обеспечивают разные стандарты для того, чтобы деяние квалифицировалось как кибертерроризм. Чтобы преодолеть это препятствие в глобальной совместной стратегии кибербезопасности, необходимо предпринять следующие шаги:

Государства должны принять универсально приемлемое определение кибертерроризма. Это гарантирует, что стандарты для акта, равнозначного кибертерроризму, будут одинаковыми во внутреннем законодательстве каждой страны. Таким образом, действие, равнозначное кибертерроризму в одной стране, также будет равносильно кибертерроризму в другой. Следовательно, если страна становится жертвой кибертеррористической атаки, исходящей из другой страны, то страна, подвергшаяся нападению, может использовать правовые инструменты другой страны для наказания виновных (виновников) или даже экстрадиции назначенных виновных (виновников).

Государства также должны согласовать свои внутренние законы о борьбе с терроризмом друг с другом. Он обеспечит общие процедуры судебного преследования и расследования кибертерроризма и поможет в глобальной борьбе с

кибертерроризмом. Это приведет к эффективному, действенному и прозрачному механизму расследования и обмена информацией, связанной с кибертерроризмом. Помимо сотрудничества в расследованиях, это также позволит ускорить сотрудничество между правоохранительными органами разных стран для других целей, таких как программы наращивания потенциала и обучение сотрудников.

Кроме того, государства должны ускорить глобальное предотвращение кибертерроризма за счет более согласованного взаимодействия в обмене разведывательными данными, управлении кибербезопасностью, сотрудничестве в повышении готовности и устойчивости к кибербезопасности посредством взаимных договоров и других инструментов. Каждое государство должно определить международную совместную структуру кибербезопасности в качестве приоритетной области своей внешней политики.

Необходимо также приложить усилия для разработки универсально обязательного и практически осуществимого международного документа о кибертерроризме, чтобы положить конец актам кибертерроризма во всем мире. Чтобы защитить свое стратегическое киберпространство, Индия должна укреплять международное сотрудничество между другими государствами и предпринимать шаги по интернационализации своих внутренних законов о кибертерроризме.

REFERENCES

1. Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. - Washington D.C.: The White House, 2009.
2. Informational Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. -Washington D.C.: The White House, 2011.
3. Department of Defense Strategy for Operating in Cyberspace. - Washington D.C.: U.S. Department of Defense, 2011.
4. Паршин С.А., Горбачев Ю.Е., Кожанов Ю.А. Кибервойны - реальная угроза национальной безопасности. - М.: Изд-во КРАСАНД, 2011.
5. Бедрицкий А.В. Международные договорённости по киберпространству: возможен ли консенсус?.// Проблемы национальной стратегии, № 4 (13), 2012.
6. Совместное заявление об общих вызовах безопасности на рубеже XXI века (Москва, 2 сентября 1998 г.) // Дипломатический вестник МИД России, № 10,1998.
7. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Резолюция Генеральной Ассамблеи ООН A/RES/58/32 - Генеральная Ассамблея ООН: 58-я сессия, № 58/32,2003.