КИБЕРТЕРРОРИЗМ КАК УГРОЗА МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ В XXI ВЕКЕ: АНАЛИЗ МЕР ПО ПРОТИВОДЕЙСТВИЮ

Анна РЫБАКОВА

CZU: 327.88:004.7:327.57”XX” anka.ribakova@gmail.com

Cyberterrorism poses a significant threat to modern international security as terrorist groups increasingly exploit virtual space for attacks. They concentrate efforts on cyberattacks targeting critical information infrastructure, potentially leading to significant economic and social consequences. Countering cyberterrorism has become one of the foremost tasks for the international community, necessitating strengthened cybersecurity and global cooperation to effectively protect national interests and societal stability.

В современном мире, с появлением глобальной сети возникла одна из наиболее опасных разновидностей киберпреступности – кибертерроризм, который, по сравнению с традиционным терроризмом, при совершении террористических акций прибегает к новейшим достижениям науки и техники. Кибертерроризм является междисциплинарным явлением, охватывая аспекты международной безопасности, права, психологии, компьютерной безопасности, что усложняет создание единого определения для его понятия.

Термин “кибертерроризм” впервые был использован в 1980-х годах Б. Коллином, старшим исследователем Института по безопасности и разведке в Калифорнии. Согласно Коллину, кибертерроризм возникает на пересечении "реального мира" и "виртуального мира"[1, p.15]. “Реальный мир” представляет собой физическую материю, которую мы воспринимаем и используем в повседневной жизни, в то время как “виртуальный мир” символичен, это пространство, где функционируют компьютерные программы и передвигаются данные. Взаимозависимость и пересечение этих миров делают людей уязвимыми перед кибертеррористами.

Кибертерроризм представляет собой угрозу использования компьютерных технологий, Интернета, виртуального пространства в террористических целях (подготовка и финансирование террористических актов, вербовка и распространение терроризма и экстремизма в сети). Если рассматривать кибертерроризм с аспекта кибербезопасности, то стоит утверждать, что данное явление представляет собой использование компьютерных технологий для нарушения функциональности критической инфраструктуры через кибератаки, DdoS-атаки, вирусы. Таким образом, кибертерроризм является многоаспектной угрозой современности, которая затрагивает все сферы жизнедеятельности людей и требует вмешательства международного сообщества для его противодействия.

Ввиду событий 11 сентября 2001 года Аль-Каида продемонстрировала свою способность эффективно использовать Интернет для планирования и координации террористических атак. Организация использовала различные онлайн-ресурсы для сбора информации, обмена сообщениями, приобретения ложных документов и обеспечения анонимности оперативников. Этот пример показывает, что киберпланирование стало неотъемлемой частью стратегии террористов и кибертерроризм представляет реальную угрозу международной безопасности. Сегодняшняя активность Аль-Каиды в онлайн-пространстве подтверждает, что Интернет продолжает быть ключевым инструментом для вербовки, пропаганды и финансирования терроризма. [2, p.17]

Одна из самых опасных террористических организаций, ИГИЛ, активно использует Интернет для распространения своей идеологии и привлечения новых сторонников. Они используют различные онлайн-платформы и социальные сети, такие как Twitter, Facebook, YouTube, SoundCloud и WhatsApp, чтобы донести свои сообщения до мировой аудитории. Профессионально созданные видеоролики, фотографии с боев и сообщения на разных языках усиливают их пропаганду и вызывают интерес к их идеям. Комбинация открытых и закрытых каналов коммуникации делает их медиа-стратегию более эффективной и влиятельной.[3, p.744]

В контексте борьбы с кибертерроризмом международные и региональные организации активно сотрудничают, разрабатывая и внедряя меры противодействия этой угрозе. ООН играет ключевую роль в стимулировании сотрудничества между государствами и разработке международных инструментов противодействия. Инициативы, такие как CT TECH, запущенная Координационным террористическим центром ООН и Интерполом, укрепляют возможности правоохранительных органов и поддерживают государства-члены в использовании новых технологий для борьбы с кибертерроризмом.

ENISA играет также ключевую роль в обеспечении кибербезопасности в Европе, предоставляя консультации и советы по защите критической инфраструктуры. НАТО ставит перед собой цели ускорения цифровой трансформации, адаптации структуры военного управления к информационному веку и укрепления киберзащиты сетей и инфраструктуры. Хотя организация уделяет большее внимание кибербезопасности, нежели кибертерроризму, ее усилия также направлены на защиту от возможных кибератак террористов. ОБСЕ активно участвует в обеспечении безопасности ИКТ, осуществляя меры по укреплению доверия и защите критической инфраструктуры.

Анализируя подход Республики Молдова в области борьбы с кибертерроризмом, стоит отметить, что страна сталкивается с серьезным вызовом в сфере кибербезопасности из-за отсутствия необходимого законодательного и нормативного основания для борьбы с кибертерроризмом. Недостаток специализированных законов и актов, а также недостаточное внимание со стороны государственных органов к этой проблеме, создают потенциальные угрозы для на-

циональной безопасности страны. В данном случае необходимо немедленное развитие и внедрение соответствующих законодательных мер и политик, чтобы обеспечить эффективную защиту информационных систем и критической инфраструктуры страны от кибертеррористических угроз.

Для того, чтобы повысить эффективность международного сообщества по борьбе с кибертерроризмом, можно выделить следующие рекомендации:

1. Необходимо приложить усилия для разработки универсально обязательного и практически осуществимого международного документа о кибертерроризме с целью прекращения актов кибертерроризма по всему миру. Этот документ должен включать в себя четкие определения кибертерроризма, установить стандарты ответственности за кибертеррористические действия, а также предложить меры для предотвращения, пресечения и наказания таких актов.
2. Установить между государствами и международными организациями эффективные механизмы оперативного обмена информацией о планировании терактов и использовании Интернета для вербовки террористов. Для этого необходимо разработать специализированные протоколы и процедуры, обеспечивающие быструю и безопасную передачу информации между компетентными органами различных стран.
3. Создать в рамках международных и региональных организаций, таких как ООН, ОБСЕ, НАТО, ЕС, специализированные органы или комитеты для координации совместных действий по борьбе с кибертерроризмом и террористической деятельностью в онлайн-пространстве. Эти специализированные комитеты должны обладать дополнительными ресурсами и полномочиями для разработки и реализации стратегий по противодействию кибертеррористическим угрозам, а также для координации усилий между государствами-участниками и другими заинтересованными сторонами.

Библиография:

1. COLLIN, B. The Future of CyberTerrorism. *Proceedings of the 11th Annual International Symposium on Criminal Justice Issues*, The University of Illinois at Chicago, 1996.
2. State of Play: Trends in Terrorist and Violent Extremist Use of the Internet 2022, p.17
3. AL-RAWI, A. Video games, terrorism, and ISIS's Jihad 3.0. *In: Terrorism and Political Violence, vol.30, №4,* 2018, p.744.

Научный руководитель
***А. ЕЖОВ**, доктор полит. наук, доцент*