УДК 341.48/49
DOI: 10.36979/1694-500X-2024-24-11-86-90

КИБЕРТЕРРОРИЗМ КАК СПОСОБЫ ТЕРРОРИСТИЧЕСКОГО ВЛИЯНИЯ НА ПРАВОВЫЕ СИСТЕМЫ

К.А. Анварбеков, А.И. Тукубашева, С.Б. Чогулдуров

Аннотация. Рассматривается важность обеспечения информационной безопасности как неотъемлемого элемента национальной и международной безопасности государств в условиях распространения транснациональной компьютерной преступности и кибертерроризма. Проблема актуальна в свете увеличивающейся угрозы кибертерроризма, рассматриваемого как экстремальная форма экстремистской деятельности, которая представляет серьезную глобальную угрозу для общей безопасности всемирного сообщества и отдельных государств. Цель данной статьи заключается в изучении проблемы борьбы с киберпреступностью, кибертерроризмом, кибер-информационными войнами, а также в анализе организационных мер по противодействию кибертерроризму на международном и национальном уровнях. Особое внимание уделяется характеристикам кибертерроризма и его отличиям от киберпреступности. Результатом исследования является формулировка выводов и предложений по улучшению национального законодательства, регулирующего уголовную ответственность за совершение террористических актов с использованием компьютерных технологий и интернета.

Ключевые слова: терроризм; кибертерроризм; киберпреступность; кибер-информационная война.

КИБЕРТЕРРОРИЗМ УКУКТУК СИСТЕМАЛАРГА ТЕРРОРИСТТИК ТААСИР КЫЛУУ ЖОЛДОРУ КАТАРЫ

К.А. Анварбеков, А.И. Тукубашева, С.Б. Чогулдуров

Аннотация. Бул макалада трансулуттук компьютердик кылмыштуулуктун жана кибертерроризмдин жайылышынын шартында мамлекеттердин улуттук жана эл аралык коопсуздугунун ажырагыс элементи катары маалыматтык коопсуздукту камсыз кылуунун маанилүүлүгү каралат. Маселе дүйнөлүк коомчулуктун жана айрым мамлекеттердин жалпы коопсуздугуна олуттуу глобалдык коркунуч туудурган экстремисттик ишмердүүлүктүн экстремалдык түрү катары каралып жаткан кибертерроризм коркунучунун күчөшүнө байланыштуу актуалдуу. Бул макаланын максаты киберкылмыштуулук, кибертерроризм, кибер маалыматтык согуштар менен күрөшүү проблемасын изилдөө, ошондой эле эл аралык жана улуттук деңгээлде кибертерроризмге каршы күрөшүү боюнча уюштуруу чараларын талдоо болуп саналат. Кибертерроризмдин өзгөчөлүктөрүнө жана анын киберкылмыштуулуктан айырмачылыктарына өзгөчө көңүл бурулат. Изилдөөнүн жыйынтыгы компьютердик технологияларды жана интернетти колдонуу менен террордук актыларды жасагандыгы үчүн кылмыш жоопкерчилигин жөнгө салуучу улуттук мыйзамдарды өркүндөтүү боюнча корутундуларды жана сунуштарды түзүү болуп саналат.

Түйүндүү сөздөр: терроризм; кибертерроризм; кибер кылмыштуулук; кибер маалымат согушу.

CYBERTERRORISM AS WAYS OF TERRORIST INFLUENCE ON LEGAL SYSTEMS

K.A. Anvarbekov, A.I. Tukubasheva, S.B. Choguldurov

Abstract. This article discusses the importance of ensuring information security as an integral element of the national and international security of states in the context of the spread of transnational computer crime and cyber terrorism. The problem is relevant in light of the increasing threat of cyberterrorism, considered as an extreme form of extremist activity that poses a serious global threat to the general security of the world community and individual states. The

purpose of this article is to study the problem of combating cybercrime, cyberterrorism, cyber-information wars, as well as to analyze organizational measures to counter cyberterrorism at the international and national levels. Particular attention is paid to the characteristics of cyberterrorism and its differences from cybercrime. The result of the study is the formulation of conclusions and proposals for improving national legislation regulating criminal liability for committing terrorist acts using computer technology and the Internet.

Keywords: terrorism; cyberterrorism; cybercrime; cyber-information warfare.

Террористическая деятельность или терроризм, а также экстремистская деятельность или экстремизм представляют собой угрозу общественной стабильности, национальной безопасности и государственному строю любой страны, независимо от уровня ее экономического и политического развития. Экстремизм сам по себе – это очень сложное и многогранное явление, которое может проникать во все аспекты общественной жизни: культуру, экономику, политику, международные и межконфессиональные отношения. Человечество знакомо с экстремизмом с тех пор, когда власть над другими людьми стала приносить определенные материальные выгоды и, вследствие этого, стала объектом стремлений отдельных лиц, пытавшихся достичь своих целей любыми средствами. При этом их не останавливали моральные нормы, традиции, общепринятые правила поведения и интересы других людей [1].

Кибертерроризм – это форма насилия, использующая угрозы и действия в киберпространстве для достижения своих целей, таких как запугивание населения и вмешательство в работу государственных органов. Он может применять различные методы, направленные на дестабилизацию и подрыв безопасности» через использование технологий и сетей. Все это ясно показывает необходимость для правительств стран разработать стратегии кибербезопасности и защиты от кибератак. Например, Будапештская конвенция о киберпреступности стала одним из первых международных соглашений, направленных на сотрудничество в борьбе с киберпреступностью [2].

Будапештская конвенция о киберпреступности направлена на усиление сотрудничества между государствами и частным сектором в предотвращении компьютерных преступлений и защите законных интересов в области использования и развития информационных технологий. Статья 2 Конвенции обязывает государства-участники разработать соответствующее законодательство и принять меры для уголовного преследования киберпреступлений. Государства должны внедрить необходимые нормы и процедуры для выявления, расследования и привлечения к ответственности лиц, совершивших киберпреступления. Это включает меры по установлению юрисдикции, сбору и сохранению электронных доказательств, обмену информацией и сотрудничеству между правоохранительными органами [3].

В соответствии со статьей 3 Будапештской конвенции, каждое государство обязано принять законодательные и иные меры для признания и наказания за перехват компьютерных данных, не предназначенных для общего доступа, как уголовного преступления. Это требует от стран-участниц разработки законов и положений, которые устанавливают ответственность и предусматривают наказание для лиц, совершивших такие действия, включая перехват данных, передаваемых внутри или через компьютерные системы. Цель этой статьи – предотвращение нарушений конфиденциальности данных и незаконного доступа к информации в киберпространстве [4].

Одной из ключевых ролей в борьбе с киберпреступлениями выполняет Контртеррористическое Управление Совета Безопасности ООН. В резолюции № 2341 (2017 г.) Совет Безопасности ООН подчеркивает важность для государств налаживания или усиления сотрудничества с заинтересованными сторонами, включая как государственные, так и частные организации [5]. Такое сотрудничество направлено на обмен информацией и опытом для предотвращения террористических атак на критически важные объекты инфраструктуры, их защиты, смягчения последствий, расследования преступлений, реагирования на них и восстановления после нанесенного ущерба. В этом контексте также подчеркивается значимость проведения совместных

учебных мероприятий и использования соответствующих коммуникационных сетей или систем экстренного оповещения [6].

Контртеррористическое управление Организации Объединенных Наций (КТУ ООН) активно реализует ряд инициатив, направленных на применение новейших технологий. Одной из таких инициатив является использование социальных сетей для сбора информации из открытых источников и цифровых доказательств с целью борьбы с терроризмом и насильственным экстремизмом, с учетом защиты прав человека. Управление также активно делится своими экспертными знаниями о применении беспилотных летательных аппаратов (БПЛА) на международных платформах и разрабатывает другие программы в этой области [7].

В современном обществе наблюдается резкий рост угроз в сфере кибербезопасности. Ежедневно мировые СМИ сообщают о новых инцидентах. Государственные структуры и бизнес-сектор активно защищаются от волн атак, в то время как хакеры воруют средства с банковских счетов обычных граждан. В связи с этим надежная защита от цифровых угроз становится критически важной для человечества. В этом контексте важно понять суть кибербезопасности и почему она необходима каждому из нас [8].

Основная цель кибербезопасности – предотвращение кражи и компрометации данных. Программа по кибербезопасности и использованию новых технологий в ООН направлена на укрепление возможностей государств-членов и частных организаций в предотвращении кибератак со стороны террористов на критически важные объекты инфраструктуры [9]. Основная цель программы также заключается в минимизации последствий кибератак на отдельные системы и обеспечении их восстановления после атаки [10].

В резолюции ООН № 2341 (2017 г.) подчеркивается необходимость многосторонних усилий в области обеспечения защиты, охватывающих различные аспекты, такие как планирование, общественное информирование и предупреждение, оперативная координация, обмен разведывательными данными и информацией, пресечение и нейтрализация, скрининг, поиск и обнаружение, контроль доступа и проверка личности, кибербезопасность, физическая защита, управление рисками, а также обеспечение целостности и безопасности производственно-сбытовых цепочек [11]. Резолюция № 2341 (2017 г.) играет ключевую роль в повышении осведомленности о угрозах терроризма и информированности общества. Она направлена на выявление подозрительной деятельности и передачу соответствующей информации правоохранительным органам. Особое внимание уделяется расширению участия общественности и развитию государственно-частного партнерства для более эффективного противодействия потенциальным террористическим угрозам и уязвимостям. Это достигается через регулярный диалог, подготовку кадров и информационно-пропагандистские мероприятия на национальном и местном уровнях. Таким образом создается благоприятная среда для обеспечения кибербезопасности.

Также стоит различать термины «информационная безопасность» и «кибербезопасность». В своем диссертационном исследовании профессор Университета Восточного Лондона Дэниэль Шатц обратил внимание на проблемы, связанные с нечетким различением между этими терминами. В своей работе «Towards a comprehensive evidence-based approach for information security value assessment» он предложил собственное определение кибербезопасности как «подход и действия, направленные на управление рисками безопасности для защиты конфиденциальности, целостности и доступности данных и активов в киберпространстве, реализуемые организациями и государствами» [12].

Европейский Союз (ЕС) активно занимается вопросами кибербезопасности. В 2016 году ЕС принял Директиву по сетевой и информационной безопасности, известную также как Директива NIS. Она была разработана для обеспечения высокого уровня безопасности сетевых и информационных систем в странах-членах ЕС. Директива обязывает государства-члены повысить свою готовность, включая создание групп реагирования на инциденты компьютерной безопасности и установление компетентного

национального органа по вопросам сетей и информационных систем [13].

В 2019 году ЕС также принял Закон о кибербезопасности, направленный на дальнейшее укрепление защиты киберпространства в Европе. Закон о кибербезопасности ЕС 2019 года, известный как «Cyber Resilience Act» (CRA), действительно вводит обязательные требования по кибербезопасности для всех продуктов и программного обеспечения, представленных на рынке Европейского Союза. Этот закон направлен на укрепление киберстойкости (cyber resilience) и защиты информационных систем в ЕС, установив стандарты безопасности и требования к производителям и поставщикам технологий [14].

В Кыргызской Республике была принята Первая Стратегия кибербезопасности на 2019–2023 годы постановлением Правительства от 24 июля 2019 года № 369. Эта стратегия устанавливает основные направления и мероприятия для обеспечения кибербезопасности в стране на пятилетний период [15].

Целью Первой Стратегии кибербезопасности Кыргызской Республики на 2019–2023 годы было создание отечественной системы и политики кибербезопасности. Она направлена на обеспечение соответствующего уровня безопасности для граждан, бизнеса и государства, защиту их жизненно важных интересов в киберпространстве, а также обеспечение устойчивого социально-экономического развития Кыргызской Республики, включая цифровую трансформацию экономики. Для реализации данной Стратегии были достигнуты следующие результаты:

- Государственный комитет национальной безопасности Кыргызской Республики» (ГКНБ КР) был назначен уполномоченным органом в области обеспечения «кибербезопасности.
- Был создан Координационный центр по обеспечению кибербезопасности при ГКНБ КР.
- Координационный центр по обеспечению кибербезопасности получил аккредитацию CC-CERT.

Дополнительно к упомянутым мероприятиям в Кыргызстане были сделаны следующие шаги в области кибербезопасности. Учреждено Государственное агентство по защите персональных данных при Кабинете Министров Кыргызской Республики, которое является уполномоченным органом по надзору за соблюдением законодательства о персональных данных. Разработан проект Закона Кыргызской Республики «О кибербезопасности», направленный на укрепление правовой базы в области кибербезопасности.

В Уголовный кодекс Кыргызской Республики введена отдельная 40-я глава «Преступления против кибербезопасности», которая включает четыре статьи, направленные на борьбу с преступлениями в сфере кибербезопасности:

- статья 319. Несанкционированный доступ к компьютерной информации и электронным документам, в информационную систему или сеть электросвязи;
- статья 320. Создание вредоносных программных продуктов;
- статья 321. Кибер-саботаж;
- статья 322. Массовое распространение электронных сообщений.

Действительно, в Кыргызской Республике введена ответственность за нарушение законодательства о защите персональных данных, что отражает значительные усилия на законодательном уровне в области кибербезопасности. Этот шаг подчеркивает важность обеспечения защиты персональных данных граждан и укрепления правовой базы в цифровом пространстве [16].

Для дальнейшего улучшения кибербезопасности страны важно продолжать работу по трансформации нормативно-правовой базы. Это включает разработку и внедрение новых законодательных инициатив, адаптацию к изменяющейся угрозной среде в киберпространстве и повышение осведомленности общественности о киберугрозах.

Продолжение работы над улучшением нормативного обеспечения кибербезопасности будет способствовать укреплению цифровой защиты и обеспечит устойчивое развитие информационной инфраструктуры Кыргызстана [17].

В заключение, кибертерроризм и киберпреступность представляют значительные угрозы для мировой безопасности. Эффективная борьба с этими угрозами требует международного

сотрудничества, улучшенного законодательства и непрерывного внедрения новых технологий для обеспечения кибербезопасности. Это сложная задача, которая требует постоянного обновления и усилий в разработке эффективных законов и технологических решений.

Важно понимать, что обеспечение кибербезопасности несет ответственность не только для государств и международных организаций, но и для каждого пользователя интернета. Все мы можем способствовать безопасности в киберпространстве, осваивая основы кибербезопасности, использование надежных паролей и осторожное отношение к личной информации в сети.

Поступила: 05.06.24; рецензирована: 19.06.24;
принята: 21.06.24.

Литература

1. Стратегия защиты киберпространства в Кыргызстане. URL: https://digital.gov.kg/activities/strategiya-zashhity-kiberprostanstva-v-kyrgyzstane/ (дата обращения: 11.03.2024).
2. Стратегия защиты киберпространства в Кыргызстане. URL: https://digital.gov.kg/activities/strategiya-zashhity-kiberprostanstva-v-kyrgyzstane/ (дата обращения: 11.03.2024).
3. *Залужный А.Г.* Экстремизм: современные представления об общественной опасности / А.Г. Залужный, Т.Н. Беляева М.: Современное право, 2012.
4. *Римский А.В.* Экстремизм и терроризм / А.В. Римский, А.В. Артюх. URL: https://cyberleninka.ru/article/n/ekstremizm-i-terrorizm-ponyatie-i-osnovnye-formy-proyavleniya/viewer (дата обращения: 22.09.2023).
5. *Мартыненко Б.К.* Теоретико-правовые вопросы политического терроризма: на примере России конца 80–90-х гг. / Б.К. Мартыненко. URL: http://www.dslib.net/teoria-prava/teoretiko-pravovye-voprosy-politicheskogo-terrorizma.html (дата обращения: 22.05.2022).
6. *Верещагин В.Ю.* Политический и религиозный экстремизм: размышления по поводу / В.Ю. Верещагин. Ростов н/Д, 1998.
7. *Старостенко О.А.* Экстремизм как фактор снижения уровня национальной безопасности и конкурентоспособности России / О.А. Старостенко, К.А. Карташов // Международный журнал прикладных и фундаментальных исследований. 2014. № 11.
8. *Грачев А.С.* Политический экстремизм / А.С. Грачев. М.: Мысль, 1986.
9. *Мамытов Т.Б.* Религиозный и националистический экстремизм / Т.Б. Мамытов. URL: https://cyberleninka.ru/article/n/religioznyy-i-natsionalisticheskiy-ekstremizm/viewer (дата обращения: 25.08.2023).
10. *Наматов Н.А.* Религиозный экстремизм в Центральной Азии / Н.А. Наматов. URL: https://www.ca-c.org/datarus/namatov.shtml (дата обращения: 12.11.2023).
11. *Баева Л.В.* Молодежный экстремизм в современной России / Л.В. Баева. URL: https://asu.edu.ru/images/File/Publikatzii/Molod_extremizm.pdf (дата обращения: 13.12.2023).
12. *Яминева Ю.Б.* Современный мир: возрастание угроз экологического терроризма / Ю.Б. Яминева, В.Е. Хвощев. URL: https://cyberleninka.ru/article/n/ekologicheskiy-terrorizm-aktualnye-problemy-na-sovremennom-etape-osobennosti-normativno-pravovogo-regulirovaniya/viewer (дата обращения: 26.11.2023).
13. *Федоров Д.И.* Профилактика экстремизма и терроризма / Д.И. Федоров. URL: http://kotlas-city.ru/uploads/com_files/terror/04.pdf (дата обращения: 18.01.2024).
14. *Wilkinson P.* Three questions on Terrorism. Government and Oppositions / P. Wilkinson. London, 1973.
15. *Wilkinson P.* Terrorism versus Democracy / P. Wilkinson // The Liberal State Response. 2006. № 5.
16. *Wilkinson P.* Embedded Expertise and the New Terrorism / P. Wilkinson. London, 2005.
17. *Каримова М.Ш.* Противодействие международному экстремизму / М.Ш. Каримова // Евразийская интеграция: экономика, право, политика. 2020. № 4.