Список источников

1. Chappelle, A. Twitter bots, fake news and propaganda in the Qatar crisis [Electronic resource] / A. Chappelle // Al Jazeera. – Mode of access: https://www.aljazeera.com/amp/news/2018/6/4/twitter-bots-fake-news-and-propaganda-in-the-qatar-crisis. – Date of access: 15.11.2023.
2. Davidson, C. The UAE, Qatar, and the Question of Political Islam [Electronic resource] / C. Davidson // Divided Gulf: The Anatomy of a Crisis / ed. by A. Krieg. – Mode of access: https://doi.org/10.1007/978-981-13-6314-6. – Date of access: 15.11.2023.
3. Jones, M. Hacking, bots and information wars in the Qatar spat [Electronic resource] / M. Jones // The Washington Post. – Mode of access: https://www.washingtonpost.com/news/monkey-cage/wp/2017/06/07/hacking-bots-and-information-wars-in-the-qatar-spat/. – Date of access: 15.11.2023.
4. Jones, M. Propaganda, Fake News, and Fake Trends: The Weoponization of Twitter Bots in the Gulf Crisis // International Journal of Communication. – 2019. – Vol. 13. – P. 1389–1415.
5. Qatar given 10 days to meet 13 sweeping demands by Saudi Arabia [Electronic resource] // The Guardian. – Mode of access: https://www.theguardian.com/world/2017/jun/23/close-al-jazeera-saudi-arabia-issues-qatar-with-13-demands-to-end-blockade. – Date of access: 15.11.2023.

***В.А. Сошенко**, студент*
Научный руководитель – О.С. Пустошинская, кандидат политических наук, доцент
ТюмГУ (Тюмень)

ОБЕСПЕЧЕНИЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЕЙ ДОГОВОРА О КОЛЛЕКТИВНОЙ БЕЗОПАСНОСТИ

В современном мире взаимосвязанности, когда нации, экономики и общество процветают благодаря мощи технологий, защита киберпространства становится необходимым условием поддержания безопасности и стабильности. С возрастанием негативных проявлений разработок в области ИКТ киберпреступность предстает как одна из наиболее существенных угроз государственной безопасности, устойчивому развитию и мировому сообществу в целом [1, с. 97]. На сегодняшний день кибертехнологии и их использование интегрируется не только отдельными странами, но и международными военно-политическими организациями. Одной из успешно реализующих практики

по обеспечению информационной безопасности своих членов считается Организация договора о коллективной безопасности (ОДКБ).

ОДКБ первоначально создавалась для обеспечения взаимной обороны от традиционных военных угроз, и лишь в 2010 г. ОДКБ закрепила в Уставе актуальность решения проблем кибербезопасности в современную эпоху [2, с. 1]. Так, в ст. 8 Устава ОДКБ закрепилась консолидация реагирования на кризисные ситуации и объединение усилий в борьбе со всеми видами угроз коллективной безопасности, в том числе и информационной [3, p. 399].

Поскольку мир становится все более взаимосвязанным, ОДКБ признает важным компонентом своей политики в области кибербезопасности разработку понятийного аппарата и гармонизацию национальных законодательств государств в сфере обеспечения информационной и коммуникационной безопасности [4, с. 38]. Государствам-членам рекомендуется разработать и обеспечить соблюдение соответствующего законодательства, криминализирующего киберпреступления и создающего надлежащие структуры киберуправления. Принимая нормативные документы о сотрудничестве государств-членов в сфере обеспечения информационной безопасности, ОДКБ обеспечивает руководство и поддержку в разработке и внедрении этих правовых рамок [5, с. 69].

В формате ОДКБ существует согласие относительно того, что под информационной безопасностью понимается состояние защищенности личности, общества, государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве [6, с. 136]. Отмечается, что количество вызовов и угроз безопасности в мире неуклонно растет в связи с этим продолжается призыв мирового сообщества воздерживаться от неправомерного использования информационно-коммуникационных технологий для пропаганды и разжигания ненависти, а также нанесения вреда информационным ресурсам, критической инфраструктуре государств, адаптируя организацию к современной геополитической ситуации в связи с ростом агрессивности мировых держав и военно-политических блоков по отношению к Российской Федерации и нашим союзникам [8].

Милитаризация информационного пространства была отмечена в Стратегии коллективной безопасности ОДКБ на период до 2025 г. от 14 октября 2016 г. Именно ей было определено среди потенциальных угроз безопасности, применение технологий «гибридной войны», рекрутирование граждан государств-членов Организации в ряды международных террористических и религиозно-экстремистских организаций, что дает основание проводить ряд направлений по совершенствованию механизмов защиты информационного пространства и разработки мер против кибервоздействия на страны ОДКБ [8].

В контексте международного мира и безопасности за последние годы риски по поводу ИИ вызвали многочисленные опасения в связи с потенциальным внесением неопределенности в международные отношения. Глобальная конкуренция за лидерство в сфере ИКТ может ускорить гонку за автоматизированным ИИ оружием [9, с. 41]. В связи с этим ОДКБ работает на опережение в правовом измерении использования искусственного интеллекта и робототехники и их применения в летальном вооружении, в области государственного регулирования сети Интернет сфере обороны и безопасности [10]. Таким образом, ОДКБ стремится и способствует прозрачной, безопасной и ответственной информационной среде.

Политика ОДКБ предусматривает совместную работу по эффективному реагированию на киберинциденты и смягчению их последствий. Это включает в себя обмен техническим опытом, проведение совместных расследований и содействие трансграничному сотрудничеству. ОДКБ уделяет большое внимание наращиванию потенциала и подготовке кадров. Государства-члены получают поддержку и ресурсы для укрепления своих возможностей в области киберзащиты, это включает в себя учебные программы, семинары и упражнения для улучшения навыков, знаний и возможностей реагирования на инциденты [8].

ОДКБ как площадка для информационной безопасности осуществляет реальные ежегодные и достаточно эффективные скоординированные оперативно-разыскные и профилактические мероприятия по борьбе с новыми вызовами и угрозам. Так, линия работ в борьбе с производством и распространением фейках о странах-участницах ОДКБ особенно активизировалась после агрессивных информационно-пропагандистских акций против России, проводимых западными военными специалистами НАТО на территории Украины [10]. В рамках операции «ПРОКСИ» приостанавливается деятельность информационных ресурсов и блокируются информационные ссылки, наносящих ущерб национальным и коллективным интересам [6, с. 138].

Таким образом, можно сделать ряд выводов, характеризующих обеспечение информационной безопасности странами ОДКБ на 2023 г.

Во-первых, роль ОДКБ в киберзащите заключается в оказании помощи странам-членам в укреплении их киберзащиты и реагировании на кибератаки, путем предоставления странам-членам платформы для обмена информацией и опытом в области киберзащиты.

Во-вторых, политика ОДКБ в области киберзащиты особое внимание уделяет обеспечению соблюдения и правоприменения эффективных мер. ОДКБ создала механизмы мониторинга и оценки приверженности государств-членов этой информационной политике. Организация следит за соблюдением

рекомендаций государствами-членами и оперативно устраняет любые отклонения или несоблюдение требований.

В-третьих, подход ОДКБ подразумевает реалистичную платформу для обучения, тестирования в области киберзащиты, в том числе с имплементацией ведущих разработок в информационной среде. Эффективность оперативно-разыскных и профилактических мероприятий сопряжена со своевременной адаптацией к меняющемуся ландшафту кибербезопасности.

Список источников

1. Харин, В. В. Киберпреступность как угроза международной безопасности / В. В. Харин, Т. В. Плотникова // Актуальные проблемы государства и права. – 2018. – № 8. – С. 96–107.
2. О внесении изменений в Устав Организации Договора о коллективной безопасности от 7 октября 2002 года [Электронный ресурс] // Электронный фонд правовых и нормативно-технических документов. – Режим доступа: https://docs.cntd.ru/document/902395154. – Дата доступа: 13.11.2023.
3. Bordyuzha, N. The Collective Security Treaty Organization: A Brief Overview [Electronic resource] / N. Bordyuzha // OSCE. – Mode of access: https://ifsh.de/file-CORE/documents/yearbook/english/10/Bordyuzha-en.pdf. – Date of access: 13.11.2023.
4. О совершенствовании системы информационной безопасности в ОДКБ / М. А. Вус [и др.] // Власть. – 2014. – № 8. – С. 37–40.
5. Дорохина, К. М. Анализ стратегии организации Договора о коллективной безопасности в сфере противодействия терроризму / К. М. Дорохина // Вест. Моск. ун-та. Сер. 12. Политические науки. – 2018. – № 5. – С. 62–76.
6. Выходец, Р. С. Формирование системы информационно-психологической безопасности Организации Договора о коллективной безопасности / Р. С. Выходец // Евразийская интеграция: экономика, право, политика. – 2023. – № 17. – С. 132–142.
7. Стратегия коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 г. [Электронный ресурс] // Организация Договора о коллективной безопасности. – Режим доступа: http://odkb-csto.org/documents/detail.php?ELEMENT_ID=8382. – Дата доступа: 14.11.2023.
8. Puscas, I. AI and International Security: Understanding the Risks and Paving the Path for Confidence-Building Measures / I. Puscas. – Geneva : UNIDIR, 2023. – 65 p.

9. Выборный, А. Искусственный интеллект – важный элемент обеспечения национальной безопасности [Электронный ресурс] / А. Выборный // Организация Договора о коллективной безопасности. – Режим доступа: https://paodkb.org/events/anatoliy-vybornyy-iskusstvennyy-intellekt-vazhnyy-element. – Дата доступа: 13.11.2023.

10. Новый инструментарий США и НАТО для информационного и киберпротивоборства с Россией в Восточной Европе [Электронный ресурс] // РСМД. – Режим доступа: https://russiancouncil.ru/analytics-and-comments/analytics/novyy-instrumentariy-ssha-i-nato-dlya-informatsionnogo-i-kiberprotivoborstva-s-rossiey-v-vostochnoy-/. – Дата доступа: 13.11.2023.