

**KIBERTERRORIZM VA UNDAN HIMOYALANISH**

Soliyeva Shahzoda Dilshodjon qizi

Qo'qon Davlat Pedagogika Universiteti

Xorijiy til va adabiyoti yo'nalishi

Abdupattayev Xasanboy Abdurakhmonovich

Qo'qon Davlat Pedagogika Universiteti o'qituvchisi

ANNOTATSIYA. Bugungi global raqamli muhitda kiberterrorizm, ya'ni terrorchilik maqsadlarida axborot-kommunikatsiya tarmoqlaridan foydalanish, davlat va jamiyat xavfsizligi uchun katta tahdidga aylangan. Ushbu maqolada kiberterrorizm tushunchasi, uning zamonaviy media muhitida qanday namoyon bo'lishi, shuningdek undan himoyalaniş strategiyalari tahlil qilinadi. Adabiyotlar sharhi, munozara va tadqiqot natijalari orqali kiberterrorizmga qarshi kurashishda media savodxonligi, raqamli xavfsizlik va reglament roli ko'rib chiqiladi.

Kalit so'zlar: kiberterrorizm; axborot hujumlari; global media muhit; himoyalaniş strategiyalari; raqamli xavfsizlik.

KIRISH. Raqamli texnologiyalar va internetning keng tarqalishi bilan birga, terrorchilik an'anaviy shakllaridan tashqari yangi formatlarga — jumladan kiberxurujlarga — ham o'tmoqda. Kiberterrorizm deganda ko'pincha «axborot-kommunikatsiya tizimlari orqali katta zarar yetkazish, qo'rqitish yoki siyosiy maqsadlar qo'yish» tushuniladi. Misol uchun, infratuzilmaga kiritilgan hujumlar orqali jamiyatda vahima yaratish mumkin (Jarvis, Macdonald, 2014 [22]). Ushbu holatlar global media muhitida tez tarqaladi va raqobatli informatsion makonda manipulyatsiya qilish imkonini yaratadi. Shuning uchun kiberterrorizmdan samarali himoyalaniş — davlatlar, ommaviy axborot vositalari va jamoatchilik uchun dolzarb masala hisoblanadi.

ADABIYOTLAR SHARHI. Tushunchani aniqlash masalasida Laura Mayer Lux 2018-yilda kiberterrorizمنى «saboq ishi» jihatdan ko'rib chiqib, uning terrorizm va kiber jinoyat chegarasi orasidagi murakkabligini ta'kidlaydi:



«kiberterrorizm ... bu texnoloji jihatdan global va o‘zaro bog‘langan dunyoda yangi muammo» deb yozadi (Mayer Lux, 2018 [5]).

Boshqa tomondan, Lee Jarvis va Stuart Macdonald tadqiqotida 118 ta xalqaro tadqiqotchilar so‘rov natijalari asosida «kiberterrorizm qarshi kurashishda an’anaviy terrorizm bilan solishtirganda qanday farqlarga ega?» degan savolga javob izlagan (Jarvis, Macdonald, 2014, pp. 657-678 [9]). Ular kiberterrorizm tushunchasida hali ham kelishmovchiliklar borligini aniqlagan. Yana bir jihat — milliy xavfsizlik nuqtai nazarida. A.Z. Zhukov va M.A. Ogorodnikov Rossiya kontekstida kiberterrorizmni “davlat xavfsizligiga zamonaviy tahdid” deb belgilagan (Zhukov, Ogorodnikov, 2023, p. 25 [10]). Ular bu xurujlar hajmi va tezligi jihatdan an’anaviy terror tajribasidan ham o‘zga ekanligini ta’kidlaydi. Shuningdek, siyosiy jihatdan kiberjinoyatchilik va terrorchilik tarmoqlari o‘zaro kesishishi haqida yaqinda o‘tgan tahlil ham mavjud — Paquet-Clouston va hamkasblari tomonidan e’lon qilingan ishda «terror va kiberjinoyatchilik o‘rtasida vositalar, infratuzilmalar va metodlar jihatdan yaqinlashuv kuzatilmoqda» (2025 [1]). Bu jihat himoyalani sh strategiyalarini qurishda yangi yondashuvlarni talab qiladi.

MUNOZARA. Kiberterrorizmga qarshi himoyalani shda bir necha yo‘nalish ko‘tarilgan. Avvalo, ta’lim va media savodxonligi muhim deb hisoblanadi — jamoatchilik o‘ziga taqdim etilgan axborotni tanqidiy analiz qila olishi kerak. Biroq, himoyalani sh faqat shaxsga yuklab qo‘yilgan mas’uliyat emas; platformalar, davlat organlari va xalqaro hamkorlik ham rol o‘ynaydi. Jarvis va Macdonald tadqiqoti respondentlari orasida «kiberterrorizm mutlaqo alohida xavfmi yoki eski terrorizm formatining qulayroq raqamli manifestatsiyasi?» degan savol bo‘yicha ham fikrlar turlicha ekanligini ko‘rsatgan (Jarvis, Macdonald, 2014 [9]). Boshqa tomondan, himoyalani shni texnologik platforma reformasi orqali ko‘rib chiqish mumkin — algoritmlar shaffofligi, markaziy nazorat mexanizmlari, infratuzilma mustahkamligi. Masalan, kiberjinoyatchilik va terrorchilik tarmoqlari infratuzilmalardan foydalangani haqida 2025-yilgi sistemati sharhda qayd etilgan (Paquet-Clouston et al., 2025 [1]). Bu himoyalani shni faqat milliy qonunchilik bilan cheklab qo‘yib bo‘lmasligini, xalqaro huquqiy va texnik choralarga ham ehtiyoj borligini ko‘rsatadi. Ammo hamma mamlakatlar bu ehtiyojni tan olmay, resurslari yetarli emasligi sababli himoyalani shda



katta farqliliklar bor — bu esa raqobatli media makonida zaif tomonlarni vujudga keltiradi.

Shunday qilib, kiberterrorizmga kurashda himoya vositalari ning kengligi, hamkorlik darajasi va jamoatchilikning tayyorgarligi muvaffaqiyat kalitidir. Biroq, bu strategiyalarni birlashtirishda murakkabliklar va resurs cheklovlari bilan duch kelinadi.

NATIJALAR. Tahlillar natijasida quyidagi asosiy xulosalar olinadi:

1. Kiberterrorizm tushunchasi hali ilmiy hamjamiyatda to'liq konsensusga ega emas, bu esa huquqiy va operativ javoblarni murakkablashtiradi (Jarvis, Macdonald, 2014 [9]; Mayer Lux, 2018 [5]).

2. Kiberjinoyatchilik va terrorchilik faoliyatlari orasida metodologik jihatdan kesishuvlar mavjud bo'lib, ular himoyalani sh strategiyalarini yangilashni talab qiladi (Paquet-Clouston et al., 2025 [1]).

3. Milliy xavfsizlik kontekstida kiberterrorizm davlatlar uchun endi faqat axborot xavfsizligi emas, balki geosiyosiy raqobat vositasiga aylanmoqda (Zhukov, Ogorodnikov, 2023 [10]).

4. Himoyalani sh strategiyalari bir qator darajalarga ega: jamoatchilikning media savodxonligi, texnologik platformalar nazorati, huquqiy-reglament choralari va xalqaro hamkorlik — ularning barchasi birgalikda samarali.

5. Globallashuv va raqamli axborot ketma-ketligi sharoitida, axborot influentsiyasi va manipulyatsiyasi ham kiberterrorizmdan himoyalani shda e'tiborga olinishi kerak.

6. **XULOSA.** Kiberterrorizm zamonaviy axborot makonida jiddiy xavf manbai bo'lib qolmoqda. Uning himoyalani shi faqat texnik jihatdan emas, balki huquqiy, pedagogik va strategik jihatdan ham ko'rib chiqilishi lozim. Jamoatchilik media savodxonligini oshirish, platformalar algoritmik muvozanatni ta'minlash, davlatlar esa xalqaro hamkorlik va mos reglament tizimlarni yotqizish orqali raqobatli global media muhitida zaifliklardan qochishi mumkin. Kelgusida kiberterrorizmga qarshi kurashda generativ sun'iy intellekt, blokcheyn va federatsiyalashgan tahliliy tizimlar ham muhim rol o'ynashi kutilmoqda. Shuning uchun ilmiy jamoa, siyosatchilar va xavfsizlik



amaliyotchilari ushbu sohada innovatsion yechimlar ishlab chiqishni davom ettirishlari muhimdir.

ADABIYOTLAR RO'YXATI

- 1.Jarvis, L., & Macdonald, S. (2014). What is cyberterrorism? Findings from a survey of researchers. *Terrorism and Political Violence*, 27(4), 657-678. (research-portal.uea.ac.uk)
- 2.Mayer Lux, L. (2018). Defining cyberterrorism. *Revista Chilena de Derecho y Tecnología*, 7(2), 5-25. (scielo.cl)
- 3.Paquet-Clouston, M., et al. (2025). The evolving nexus of cybercrime and terrorism: A systematic review of convergence and policy implications. *Security Journal*, 38, Article 29. (link.springer.com)
- 4.Zhukov, A. Z., & Ogorodnikov, M. A. (2023). Cyberterrorism as a Modern Threat to State Security. *Criminalistic, procedural and operative-search measures to counter crime in the globalisation conditions*, 16(4), 25-29. ([Eco-Vector Journals Portal](https://eco-vector-journals.ru))
- 5.Amrullah, K. (2024). Cyberterrorism and National Security: Issues and Challenges in Contemporary Indonesia. *Indonesian Journal of Counter Terrorism and National Security*, 3(1). (journal.unnes.ac.id)
- 6.Straub, V. J. (2020). Beyond kinetic harm and towards a dynamic conceptualization of cyberterrorism. *arXiv*. ([arXiv](https://arxiv.org))