AXBOROT URUSHLARI TAHDIDLARIGA QARSHI SAMARALI STRATEGIYALARNI ISHLAB CHIQISH YO‘NALISHLARI

Muallif: ***Zaidov Azizbek Avazbekovich***

O‘zbekiston Respublikasi Jamoat Xavfsizligi
Universiteti magistratura tinglovchisi, podpolkovnik

Annotatsiya

Mazkur ilmiy maqolada globallashuv va raqamli transformatsiya sharoitida axborot urushlarining zamonaviy xavfsizlik tizimiga ta’siri chuqur tahlil qilinadi. Axborot urushlarining mohiyati, shakllari va ularning davlat hamda jamiyat barqarorligiga yetkazayotgan tahdidlari ilmiy asosda yoritiladi. Tadqiqot doirasida axborot urushlari tahdidlariga qarshi samarali strategiyalarni ishlab chiqishning huquqiy, institutsional, texnologik, axborot-ma’naviy va xalqaro hamkorlik yo‘nalishlari kompleks yondashuv asosida ochib beriladi. Maqolada ilmiy yangilik sifatida axborot urushlariga qarshi ko‘p darajali milliy strategik model taklif etilib, uni amaliyotga tatbiq etish bo‘yicha aniq taklif va tavsiyalar ilgari suriladi.

Kalit so‘zlar: axborot urushi, axborot xavfsizligi, milliy xavfsizlik, dezinformatsiya, kiberxavfsizlik, strategiya.

Аннотация

В данной научной статье всесторонне анализируется влияние информационных войн на современную систему безопасности в условиях глобализации и цифровой трансформации. Научно обоснованно раскрываются сущность и формы информационных войн, а также угрозы, которые они

создают для устойчивости государства и общества. В рамках исследования на основе комплексного подхода рассматриваются правовые, институциональные, технологические, информационно - духовные и международные направления разработки эффективных стратегий противодействия угрозам информационных войн. В качестве научной новизны в статье предлагается многоуровневая национальная стратегическая модель противодействия информационным войнам, а также выдвигаются конкретные рекомендации по её практической реализации.

Ключевые слова: информационная война, информационная безопасность, национальная безопасность, дезинформация, кибер безопасность, стратегия.

Abstract

This scientific article provides an in-depth analysis of the impact of information warfare on contemporary security systems under the conditions of globalization and digital transformation. The essence and forms of information warfare, as well as the threats they pose to the stability of the state and society, are examined on a scientific basis. Within the framework of the study, effective strategies for countering information warfare threats are explored through a comprehensive approach encompassing legal, institutional, technological, informational–cultural, and international cooperation dimensions. As a scientific contribution, the article proposes a multi-level national strategic model for countering information warfare and puts forward specific recommendations for its practical implementation.

Keywords: information warfare, information security, national security, disinformation, cybersecurity, strategy.

XXI asrda globallashuv, raqamli texnologiyalar va axborot-kommunikatsiya vositalarining jadal rivojlanishi axborotni strategik resurs darajasiga olib chiqdi. Davlatlar o‘rtasidagi raqobat faqat harbiy yoki iqtisodiy sohada emas, balki axborot makonida ham kechmoqda. Axborot makoni jamiyat ongi, ijtimoiy barqarorlik va milliy xavfsizlikka ta’sir etuvchi muhim omilga aylandi [1].

Zamonaviy axborot urushlari ochiq harbiy to‘qnashuvlarsiz, ko‘pincha tinchlik davrida, yashirin va gibrid shakllarda amalga oshirilishi bilan tavsiflanadi. Ular orqali jamoatchilik fikri manipulyatsiya qilinadi, ijtimoiy ishonch susaytiriladi va davlat institutlarining legitimligiga putur yetkaziladi [2].

Shu bois, axborot urushlari tahdidlariga qarshi samarali strategiyalarni ishlab chiqish milliy xavfsizlikni ta’minlashda dolzarb ilmiy va amaliy masala hisoblanadi.

Axborot urushi tushunchasi ilmiy adabiyotlarda turlicha talqin qilinadi. Amerikalik olim M. Libicki axborot urushini raqib tomonning axborot to‘plash, qayta ishlash va qaror qabul qilish qobiliyatiga ta’sir ko‘rsatishga qaratilgan harakatlar majmui sifatida izohlaydi [3].

Rossiyalik tadqiqotchilar esa axborot urushini davlatning ma’naviy-mafkuraviy xavfsizligiga qarshi qaratilgan tizimli ta’sir sifatida baholaydilar [4].

Ilmiy yondashuvlarga ko‘ra, axborot urushlarining asosiy xususiyatlari quyidagilardan iborat:

- harbiy kuch qo‘llanilmasdan amalga oshirilishi;
- ommaviy axborot vositalari va raqamli platformalarga tayanilishi;
- jamiyat ongi va qadriyatlar tizimiga yo‘naltirilganligi.

Zamonaviy axborot urushlari quyidagi asosiy shakllarda namoyon bo‘ladi:

1. Dezinformatsiya va fake axborotlar
Soxta axborotlar orqali jamoatchilik fikrini chalg‘itish va ijtimoiy beqarorlikni kuchaytirish axborot urushlarining eng keng tarqalgan usullaridan biridir. Yevropa Ittifoqi tadqiqotlariga ko‘ra, dezinformatsiya kampaniyalari saylov jarayonlari va ijtimoiy barqarorlikka bevosita ta’sir ko‘rsatadi [5].

2. Kiberhujumlar
DDoS, phishing, zararli dasturlar orqali davlat axborot tizimlari va muhim infratuzilmalarga zarar yetkaziladi. 2007-yilda Estoniyada sodir bo‘lgan kiberhujumlar buning yaqqol misolidir [6].

3. Psixologik va mafkuraviy ta’sir
Ijtimoiy tarmoqlar orqali maqsadli auditoriyaga psixologik bosim o‘tkazish, radikal g‘oyalarni singdirish amalga oshiriladi [7].

4. Sun’iy intellektga asoslangan hujumlar
Deepfake, bot-tarmoqlar va avtomatlashtirilgan manipulyatsiya mexanizmlari axborot urushlarining yangi bosqichini yuzaga keltirmoqda [8].

2007-yilda Estoniya davlati global miqyosdagi DDoS (Distributed Denial of Service — taqsimlangan xizmatdan mahrum etish) hujumlariga uchradi, ya’ni bir vaqtning o‘zida ko‘plab manbalar (kompyuterlar, serverlar, bot-tarmoqlar) orqali belgilangan server yoki veb-xizmatga katta hajmda so‘rov yuborilishi natijasida tizim ortiqcha yuklanib, qonuniy foydalanuvchilar uchun xizmat ko‘rsata olmay qoldi. Ushbu hujumlar davlat organlari, bank tizimi va telekommunikatsiya infratuzilmasini to‘xtatdi.

Yuqoridagi kabi holatlarning oldini olish maqsadida “e-Estonia” raqamli davlat modeli yaratilib, Estoniya kiberxavfsizlik bo‘yicha yetakchi davlatga aylandi [6].

AQShda kiberxavfsizlik davlat va xususiy sektor hamkorligiga asoslangan bo‘lib, CISA (Cybersecurity and Infrastructure Security Agency — Kiberxavfsizlik va infratuzilma xavfsizligi agentligi) milliy kiberxavfsizlikni ta’minlab, muhim infratuzilmalarni (energetika, transport, aloqa, moliya tizimlari) himoya qiladi. NSA (National Security Agency — Milliy xavfsizlik agentligi) maxsus razvedka organi bo‘lib, axborot razvedkasi, kiberxavfsizlik va milliy xavfsizlikka oid elektron ma’lumotlarni himoyalaydi hamda tahlil qiladi. Shuningdek, FBI (Federal Bureau of Investigation — Federal tergov byurosi) federal darajadagi huquqni muhofaza qiluvchi organ bo‘lib, kiberjinoyatlar, terrorizm, davlat xavfsizligiga tahdidlar va og‘ir jinoyatlarni tergov qiladi.

Global kiberxavfsizlik sohasida yetakchi hisoblangan AQShda kiberhujumlar va ma’lumot o‘g‘irlanishiga qarshi ilg‘or tizimlar ishlab chiqilib, juda keng qamrovli faoliyat olib boriladi [9].

Xitoyda kiberxavfsizlik davlat nazorati ostida bo‘lib, axborot makoni va infratuzilmani himoya qilishga qaratilgan. Hukumatning bu borada qo‘llagan samarali strategiyalari quyidagilardan iborat:

- 2017-yilda qabul qilingan “Cybersecurity Law” — milliy kiberxavfsizlik to‘g‘risidagi qonunchilik;
- internet infratuzilmasini milliy darajada nazorat qilish;
- kiberhujumlar va dezinformatsiyaga qarshi milliy monitoring olib borish;
- sun’iy intellekt va katta ma’lumotlar orqali tahdidlarni aniqlash [10].

Rossiyada kiberxavfsizlik milliy xavfsizlikning ajralmas qismi sifatida qaralib, Roskomnadzor, FSTEC kabi davlat kiberxavfsizlik agentliklari va markazlari tomonidan kritik infratuzilmalarni himoya qilish, DDoS hujumlarini

oldini olish, milliy kiberharbiy kuchlarni rivojlantirish hamda axborot urushi va dezinformatsiya kampaniyalariga qarshi maxsus chora-tadbirlar qo‘llash orqali kiberxavfsizlik ta’minlanadi [11].

Zamonaviy nazariyalarga ko‘ra, axborot makonidagi tahdidlar gibrid xususiyatga ega bo‘lib, ular bir vaqtning o‘zida ham harbiy, ham siyosiy, ham kiberxavfsizlik xavflarini o‘z ichiga oladi. Bu esa kompleks strategiyalarni ishlab chiqish zaruratini keltirib chiqaradi.

Axborot urushlariga qarshi samarali strategiyalarni ishlab chiqish yo‘nalishlari:

Huquqiy yo‘nalishda – kiberjinoyatlarga qarshi qonunchilikni kuchaytirish, xalqaro me’yorlarni milliy qonunchilikka integratsiya qilish zarur [12].

Institutsional yo‘nalishda – maxsus kiberxavfsizlik markazlari, CERT va SOC tuzilmalarini rivojlantirish muhim ahamiyatga ega.

Texnologik yo‘nalishda – Firewall, IDS/IPS, kriptografik himoya, sun’iy intellekt asosidagi monitoring tizimlarini joriy etish [13].

Axborot - ma’naviy yo‘nalishda – media savodxonlikni oshirish, tanqidiy fikrlashni rivojlantirish va milliy axborot immunitetini shakllantirish [14].

Axborot urushlari transmilliy xususiyatga ega bo‘lganligi sababli, xalqaro hamkorlik muhim ahamiyat kasb etadi. Jahon tajribasi shuni ko‘rsatmoqdaki, axborot urushlarini bartaraf etish hamda kiberxavfsizlikni ta’minlash uchun milliy choralarni o‘zi yetarli emas. Shu sababli NATO, Yevropa Ittifoqi, ShHT kabi tuzilmalarda kiberxavfsizlik bo‘yicha quyidagi yo‘nalishlarda qo‘shma strategiyalar ishlab chiqish zarur bo‘lib qolmoqda [4]:

- xalqaro huquqiy mexanizmlarni yaratish;

- transchegaraviy kiberxavfsizlik standartlarini amalga oshirish;
- qo‘shma monitoring tizimlarini ishlab chiqish.

Ushbu model axborot urushlari tahdidlariga tizimli va barqaror qarshi turish imkonini beradi.

Xulosa qilib aytganda, axborot urushlari zamonaviy milliy xavfsizlik tizimining ajralmas muammosiga aylandi. Ularga qarshi kurashish texnik choralar bilangina cheklanmasdan, huquqiy, institutsional, ma’naviy va xalqaro yondashuvlarni o‘z ichiga olgan kompleks strategiyani talab etadi. Mazkur maqolada ishlab chiqilgan ilmiy xulosalar va takliflar axborot xavfsizligini ta’minlash amaliyotida muhim nazariy asos bo‘lib xizmat qiladi deb umid qilamiz.

FOYDALANILGAN ADABIYOTLAR

1. Castells M. The Rise of the Network Society. Wiley-Blackwell, 2010.
2. Nye J. Cyber Power. Harvard Kennedy School, 2010.
3. Libicki M. What Is Information Warfare? RAND, 1995.
4. Панарин И.Н. Информационная война и геополитика. Москва, 2012.
5. European Commission. Tackling Online Disinformation.
6. NATO CCDCOE. Cyber Attacks Against Estonia (2007).
7. UNESCO. Journalism, Fake News & Disinformation.
8. European Union. Artificial Intelligence and Disinformation.
9. U.S. Department of Homeland Security – CISA.

10. Cybersecurity Law of the PRC (2017).

11. Russian Federation Information Security Doctrine.

12. Council of Europe. Budapest Convention on Cybercrime.

13. ISO/IEC 27001:2022.

14. OECD. Media Literacy in the Digital Age.

15. NATO. Countering Hybrid Threats.