

RAQAMLI TARG'IBOT TEXNOLOGIYALARINING IMKONIYATLARI (AQSh misolida)

Maftuna Raxmonovna Xalilova

Doniyorbek Baxromjon o'g'li Abduvaliyev

“TIQXMMI” Milliy tadqiqot universitetining Qarshi irrigatsiya va agrotexnologiyalar instituti

ANNOTATSIYA

Mazkur maqolada raqamli targ'ibot texnologiyalarining imkoniyatlari AQSH misolida tahliliy bayon etildi. Unda kibertahdid masalasiga urg'u berildi. Internet tahdidi bugungi kunda davlatlar o'rtasida kelib chiqayotgan nizolarni sabab bo'lishi asoslandi.

Kalit so'zlari: kibertahdid, texnologiya, targ'ibot, internet, kiberurush, mafkura, ma'naviyat, g'o'ya, davlat, milliy mintalitet, etnik guruh, tahdid.

ABSTRACT

In this article, the possibilities of digital advertising technologies were analytically presented on the example of the United States of America. It emphasized the issue of cyber threats. The threat of the Internet is considered to be the cause of conflicts between countries today.

Keywords: cyber threat, technology, propaganda, internet, cyber war, ideology, spirituality, idea, state, national mentality, ethnic group, threat.

АННОТАЦИЯ

В данной статье аналитически представлены возможности цифровых рекламных технологий на примере Соединенных Штатов Америки. Особое внимание было уделено проблеме киберугроз. Угроза Интернета сегодня считается причиной конфликтов между странами.

Ключевые слова: киберугроза, технология, пропаганда, интернет, кибервойна, идеология, духовность, идея, государство, национальный менталитет, этнос, угроза.

Kirish

Axborot olami ichida yashayotgan bugungi kun kishisi umri davomida ko'pdan-ko'p manbalar, dalillar raqamlarga murojaat qilishga majbur. “Raqamlar sehri”dan insonlarni ta'sir doirasiga olishning bir usuli sifatida foydalanilishi ham shundan. Aslida, bu narsalar insonga

atrofda – yurtida va dunyoda sodir bo'layotgan voqea, hodisa, jarayonlarni anglashi, ularning o'zaro aloqadorligi, munosabati va mohiyatiga chuqur kirib borishi uchun kerak. Bugun oddiy ma'naviyat bilan ilg'orlar safida bo'lish ehtimoli past. Bu yerda faqat yuksak ma'naviyatgina yordam bera oladi.

Raqamli dunyo ko'rinadigan va hozirgi tahdidning yangi turini olib keldi, ya'ni kiber urushni vujudga keltirmoqda. Internet va axborot texnologiyalari shu darajada rivojlanganki, ular hozir milliy kuchning asosi bo'lib ko'rinadi, so'nggi yillarda kiber urush tobora ortib borayotgan sarlavhalarni bosib o'tib, bu muammoning ko'lamini ko'rsatmoqda. Mamlakatlar o'zlarining kiber salohiyatini kuchaytirayotgan, milliy kiberxavfsizlik strategiyalarini ishlab chiqarayotgan va ayni paytda yangi siyosiy motivlarga ega kibermudofaa va hujum vositalarini qidirayotgan paytda kibermakon siyosiy mojarolarning yangi maydoniga aylandi.

Mavzuga oid adabiyotlar tahlili (Literature review). Kiber urushning umum e'tirof etilgan ta'rifi yo'q. Richard A. Klark, ilgari AQSh xavfsizlik, infratuzilmani himoya qilish va terrorizmga qarshi kurash bo'yicha milliy koordinator va eng ko'p sotilgan “Kiber urush: Milliy xavfsizlikka keyingi tahdid va unga qarshi nima qilish kerak” nomli kitobining hammuallifi kiber urushni “millatning harakatlari” deb ta'riflaydi. U bir davlat boshqa davlatning kompyuterlari yoki tarmoqlariga zarar yetkazishi yoki buzish maqsadida kirib borishini tushuntiradi. Bugun jamiyatimizda raqamli texnologiyalarning ahamiyati tobora ortmoqda. Ularning keng joriy qilinishi va raqamli iqtisodiyotni rivojlantirish masalalari hozirgi zamonda har bir davlat uchun jiddiy hayotiy masalaga aylangan. Ekspertlar fikricha, kelgusi 3 yilda iqtisodiyotni raqamlashtirish orqali dunyodagi 22 foiz ish o'rni axborot texnologiyalari yordamida yaratiladi. Prezidentimizning Oliy Majlisga Murojaatnomasida raqamli iqtisodiyotga faol o'tish kelgusi 5 yildagi eng ustuvor vazifalardan biri sifatida belgilandi. Shuningdek, 2020 yilni Ilm, ma'rifat va raqamli iqtisodiyotni rivojlantirish yili deb e'lon qilingani bejiz emas. Raqamli iqtisodiyot, birinchi navbatda, korrupsiyadan xoli hududda ishlash imkoniyatini yaratadi.

Tadqiqot metodologiyasi (Research Methodology). Hozirgi vaqtda yangi tendensiya yangi yo'nalishni ko'rsatmoqda. To'g'ridan-to'g'ri hujumlardan jamiyatga qarshi harakatlarga, ishontirishga qaratilgan hujumlarga o'tmoqda. Natijada tashviqot kiber urushning muhim elementiga aylanib bormoqda. Kibertahdid mavzusini o'rganayotgan ko'plab tadqiqotchilar bor. Jeffri Karrning fikriga ko'ra, yashirin kiber harakatlar ikkita umumiy turdagi bo'lishi mumkin: - maqsadli mamlakatning muhim elementlarini qo'llab-quvvatlovchi nodavlat aktyorlarning kompyuter tarmoqlarini falaj qilish harakatlari; - psixologik operatsiyalar ostida qoladigan targ'ibot va dezinformatsiya.

Tahlil va natijalar (Analysis and results). Yuqorida ta’kidlanganidek, kiber arenadagi tashviqot hukumatlar tomonidan boshqa mamlakatlarning siyosiy, iqtisodiy yoki harbiy sharoitlariga urush quroli sifatida ta’sir qilish uchun foydalanilayotganini isbotlaydi. Hukumatlar yolg’on ma’lumotlarni tarqatish va ijtimoiy fanlarning aqlli taktikalarini qo’llash orqali bostirib kirish, aldash va nazorat qilish maqsadida yashirin onlayn operatsiyalarni amalga oshirmoqda.

Xulosa va takliflar (Conclusion/Recommendations). Xulosa qilib aytganda, bugungi kunda AQSh federal idoralar va idoralarning asosiy vazifalari doimiy xavf ostida qolishi mumkin. Kiberkosmosning raqamli jang maydonlarida tahdid sub’ektlari ustunlik qiladi va nafaqat “gov” muhitini, balki AQSh agentliklar xizmat ko’rsatadigan infratuzilma, sanoat va shaxslarni ham urmoqda. Biroq, kiberhujumlar tobora tez-tez va shiddatli o’sib borayotgan bo’lsa ham, bu muhim institutlar eski infratuzilma, maxsus muvofiqlashtirish va reaktiv kibernudofaa operatsiyalari kabi muammolar bilan bog’liq. Yildan-yilga gov kiberxavfsizlikka bag’ishlangan xarajatlarning sezilarli o’sishi kiberxavfsizlikning nisbatan yetukligini oshirdi, ammo gov ekotizimini davom etayotgan hujumdan himoya qila olmadi.

ADABIYOTLAR

1. Gerasimov V. Zadachi Voennoy Nauki, Obzor voyenno-politicheskoy obstanovkimire, http://dokwar.ru/publ/novosti_i_sobytiya/mnenie/zadachi_voennoj_nauki/9-1-0-681 (retrieved 02.02.2015)
2. Sommer P., Brown I., Reducing Systemic Cybersecurity Risk 2011 - 6 p
3. Suciu P., Why cyber warfare is so attractive to small nations Article, Fortune, 2014
4. Geers K., Cyberspace and the changing nature of warfare, SC Magazine, 2008
5. Applegate S.D., "National Security Special Focus: Cyber Warfare." Center for the Study of Technology and Society. Washington D.C., 2001 – p. 10
6. Carr J, Inside Cyber Warfare. Mapping the Cyber Underworld, O’Reilly 2nd edition, 2012
7. Booz Allen Hamilton. [American City Business Journals](https://www.boozallen.com/insights/cyber/transforming-federalcybersecurity.htm). 2022 yil 2-soni. <https://www.boozallen.com/insights/cyber/transforming-federalcybersecurity.htm>