

KIBERTAHDIDLARNING YOSHLAR ONGIGA TA’SIRI VA KIBERMADANIYAT HIMOYA OMILI SIFATIDA

Boymirzayev Qobil Karimjonovich

Namangan davlat universiteti mustaqil tadqiqotchisi (PhD)

DOI: <https://doi.org/10.5281/zenodo.23396573>

Annotatsiya. Maqolada raqamli muhitdagi kibertahdidlarning yoshlar ongiga ta’sir mexanizmlari ijtimoiy-falsafiy jihatdan tahlil qilinadi. U.Bekning xavf jamiyati konsepsiyasi, D.Kanemanning ikki tafakkur tizimi nazariyasi va R.Chaldinining ta’sir tamoyillari asosida kibertahdidlarning iqtisodiy-firibgarlik, kommunikativ-psixologik, g’oyaviy-manipulyativ va jinoiy jalb etish turlaridan iborat tipologiyasi ishlab chiqilgan. Kibertahdidlar texnik tizimlarga emas, balki inson ongidagi zaifliklarga yo’naltirilgani asosanib, kibermadaniyat kognitiv filtr, irodaviy to’xtam va ijtimoiy tayanchdan iborat “raqamli immunitet” sifatida talqin etilgan.

Kalit soʻzlar: kibertahdid, kibermadaniyat, yoshlar ongi, ijtimoiy muhandislik, xavf jamiyati, raqamli immunitet, kiberbulling, onlayn firibgarlik, profilaktika

ВЛИЯНИЕ КИБЕРУГРОЗ НА СОЗНАНИЕ МОЛОДЁЖИ И КИБЕРКУЛЬТУРА КАК ФАКТОР ЗАЩИТЫ

Аннотация. В статье с социально-философских позиций анализируются механизмы воздействия киберугроз цифровой среды на сознание молодежи. На основе концепции общества риска У.Бека, теории двух систем мышления Д.Канемана и принципов влияния Р.Чалдини разработана типология киберугроз, включающая экономико-мошеннические, коммуникативно-психологические, идейно-манипулятивные угрозы и вовлечение в преступную деятельность. Обосновано, что киберугрозы направлены не на технические системы, а на уязвимости человеческого сознания, а киберкультура интерпретируется как «цифровой иммунитет», состоящий из когнитивного фильтра, волевой паузы и социальной опоры.

Ключевые слова: киберугроза, киберкультура, сознание молодежи, социальная инженерия, общество риска, цифровой иммунитет, кибербуллинг, онлайн-мошенничество, профилактика

THE IMPACT OF CYBER THREATS ON YOUNG PEOPLE’S MINDS AND CYBERCULTURE AS A PROTECTIVE FACTOR

Abstract. The article provides a socio-philosophical analysis of the mechanisms by which cyber threats in the digital environment affect youth consciousness. Drawing on U. Beck’s risk society concept, D. Kahneman’s theory of two systems of thinking, and R. Cialdini’s principles of influence, a typology of cyber threats is developed, comprising economic-fraudulent, communicative-psychological, ideological-manipulative threats and recruitment into criminal activity. It is substantiated that cyber threats target vulnerabilities of human consciousness rather than technical systems, and cyberculture is interpreted as a “digital immunity” consisting of a cognitive filter, a volitional pause, and social support.

Keywords: cyber threat, cyberculture, youth consciousness, social engineering, risk society, digital immunity, cyberbullying, online fraud, prevention

KIRISH

Raqamli texnologiyalar yoshlar uchun ta'lim, ijod va o'zini namoyon etishning cheksiz imkoniyatlarini ochish bilan birga, ularni ilgari ma'lum bo'lmagan xavf-xatarlar bilan ham to'qnashtirmoqda. Onlayn firibgarlik, shaxsiy ma'lumotlarni o'g'irlash, kiberbulling, soxta axborot va yoshlarni internet orqali g'ayriqonuniy faoliyatga jalb qilish kabi tahdidlar kundalik voqelikka aylandi. Bu tahdidlarning o'ziga xos jihati shundaki, ularning aksariyati murakkab texnik hujumlar orqali emas, balki inson ishonuvchanligi, qiziquvchanligi, qo'rquvi yoki moddiy manfaatga intilishidan foydalanish orqali amalga oshiriladi. Shu sababli kibertahdidlar faqat texnik muammo emas, balki chuqur ijtimoiy-falsafiy va ma'naviy muammodir.

O'zbekistonda kiberxavfsizlik sohasidagi munosabatlarni tartibga soluvchi maxsus qonun qabul qilingan [1], raqamli transformatsiya strategiyasida axborot xavfsizligini ta'minlash muhim yo'nalish sifatida belgilangan [2]. Bolalarni zararli axborotdan himoya qilishning huquqiy asoslari ham mavjud [3]. Biroq huquqiy va texnik choralar foydalanuvchining o'zi tahdidni anglay olmasa yetarli himoya bera olmaydi. Yoshlarni zararli ta'sirlardan himoya qilish davlat siyosatining ustuvor vazifasi ekani [4] kibertahdidlarga qarshi kurashda inson omiliga e'tiborni kuchaytirishni taqozo etadi.

Maqolaning maqsadi — kibertahdidlarning yoshlar ongiga ta'sir mexanizmlarini ijtimoiy-falsafiy jihatdan ochib berish va kibermadaniyatning himoya omili sifatidagi rolini asoslashdan iborat. Vazifalar: kibertahdidlarning tipologiyasini ishlab chiqish; ularning ongga ta'sir mexanizmlarini aniqlash; kibermadaniyatning himoya mexanizmlarini asoslash va profilaktikani takomillashtirish bo'yicha takliflar ishlab chiqish.

TADQIQOT METODOLOGIYASI

Tadqiqotda dialektik, tizimli-strukturaviy, tipologik, qiyosiy-tahliliy va kontent-tahlil metodlaridan foydalanildi. Tipologik metod turli kibertahdidlarni ta'sir obyekti va mexanizmiga ko'ra tasniflashda, tizimli yondashuv kibermadaniyatning himoya mexanizmlarini yaxlit model sifatida ishlab chiqishda qo'llanildi. Ochiq manbalardagi kiberfiribgarlik holatlari va ogohlantirish materiallari kontent-tahlil asosida umumiy tarzda o'rganildi, xorijiy empirik tadqiqotlar natijalari qiyosiy tahlil qilindi.

Nazariy-metodologik asosni U.Bekning xavf jamiyati konsepsiyasi [5], D.Kanemanning “tez” va “sekin” tafakkur tizimlari haqidagi nazariyasi [6], R.Chaldinining ijtimoiy ta'sir tamoyillari [7], J.Sulerning onlayn tormozsizlanish effekti haqidagi tadqiqoti [8], kiberbulling oqibatlariga oid meta-tahlil natijalari [9] hamda J.Roozenbek va S. van der Lindenning “axborot emlash” tadqiqoti [10] tashkil etdi.

NATIJALAR

1. Kibertahdidlar tipologiyasi.

Tahlil natijasida yoshlar ongiga ta'sir etuvchi kibertahdidlarni ta'sir maqsadi va mexanizmiga ko'ra to'rt turga ajratish mumkinligi aniqlandi (1-jadval). Jadvalda har bir tahdid ongning qaysi zaifligidan foydalanishi va kibermadaniyat unga qarshi qanday himoya mexanizmini taklif etishi ko'rsatilgan.

1-jadval. Kibertahdidlar tipologiyasi va kibermadaniyatning himoya mexanizmlari

Tahdid turi	Namoyon bo‘lish shakllari	Foydalaniladigan zaiflik	Kibermadaniyatning himoya mexanizmi
Iqtisodiy-firibgarlik	Fishing xabarlarini, soxta yutuq va investitsiya takliflari, karta ma’lumotlarini qo‘lga kiritish	Ishonuvchanlik, “oson pul” illyuziyasi, shoshilinchlik bosimi	Kognitiv filtr: firibgarlik belgilarini tanish; “to‘xta va tekshir” odati
Kommunikativ-psixologik	Kiberbulling, shaxsiy materiallar bilan shantaj qilish, tahqirlash	Ijtimoiy e’tirofga ehtiyoj, uyat va qo‘rquv hissi	Ijtimoiy tayanch: kattalarga va vakolatli organlarga murojaat qilish madaniyati
G‘oyaviy-manipulyativ	Soxta axborot, radikal g‘oyalar targ‘iboti, soxta video va tasvirlar	Hissiy reaksiya, tanqidiy tafakkur yetishmasligi, o‘zlikni izlash	Kognitiv filtr: manbani tekshirish, manipulyatsiya usullarini anglash
Jinoiy jalb etish	Bank kartasini “ijaraga berish”, kuryerlik, ma’lumotlarni sotish takliflari	Moddiy ehtiyoj, javobgarlikni anglamaslik	Irodaviy to‘xtam va huquqiy ong: oqibatni anglash, taklifni rad etish

2. Kibertahdidlarning ongga ta’sir mexanizmi.

Tahlil kibertahdidlarning asosiy nishoni texnik tizim emas, balki inson ongi ekanini ko‘rsatdi. D.Kaneman inson tafakkurida ikki tizimni ajratadi: birinchi tizim tez, avtomatik va hissiyotga asoslangan, ikkinchi tizim esa sekin, mantiqiy va diqqat talab qiladigan tafakkurdir [6]. Kiberfiribgarlarning deyarli barcha usullari birinchi tizimni faollashtirib, ikkinchisini “o‘chirib qo‘yish”ga qaratilgan: “hisobingiz bloklanadi”, “faqat bugun”, “tezda tasdiqlang” kabi xabarlar shoshilinchlik va qo‘rquv uyg‘otib, insonni o‘ylab ko‘rishdan oldin harakat qilishga undaydi. R.Chaldini ta’riflagan ta’sir tamoyillari — obro‘ga bo‘ysunish, tanqislik, ijtimoiy isbot va o‘zaro javob qaytarish [7] ijtimoiy muhandislik hujumlarida tizimli ravishda qo‘llaniladi: firibgar o‘zini bank xodimi yoki davlat idorasi vakili deb tanishtiradi, “cheklangan imkoniyat” haqida xabar beradi yoki “boshqalar allaqachon foyda ko‘rgan”ini ta’kidlaydi.

Yoshlarning ushbu tahdidlarga nisbatan zaifligini oshiruvchi qo‘shimcha omillar ham mavjud. J.Suler ko‘rsatganidek, onlayn muhitdagi anonimlik va masofa insonning xulq-atvoridagi ichki to‘siqlarni zaiflashtiradi [8]. Bu holat yoshlarni bir tomondan tajovuzkor xatti-harakatlarga, masalan, kiberbullingga undasa, ikkinchi tomondan notanish shaxslarga haddan tashqari ochiqlik ko‘rsatishga olib keladi. Kiberbullingga oid meta-tahlil natijalari uning yoshlarning ruhiy holati, o‘ziga bo‘lgan bahosi va ijtimoiy moslashuviga jiddiy salbiy ta’sir ko‘rsatishini tasdiqlaydi [9].

3. Xavf jamiyatida kibermadaniyatning o‘rni.

U.Bek zamonaviy jamiyatni “xavf jamiyati” sifatida tavsiflab, unda xavflar tabiat emas, balki insonning o‘zi yaratgan texnologiyalar mahsuli ekanini va xavflarni boshqarish mas’uliyati tobora ko‘proq har bir shaxsga yuklanayotganini ko‘rsatadi [5]. Kibermakon bu tendensiyaning yorqin ifodasidir: davlat, bank va platformalar qanchalik himoya choralari ko‘rmasin,

foydalanuvchi bir lahzalik ehtiyotsizligi bilan bu himoyani bekor qilishi mumkin. Shu sababli kibermadaniyat zamonaviy xavf jamiyatida shaxsning asosiy himoya resursiga aylanadi.

4. Kibermadaniyat “raqamli immunitet” sifatida.

Tahlil asosida kibermadaniyatni uch qatlamli “raqamli immunitet” sifatida talqin qilish taklif etiladi. Birinchi qatlam — kognitiv filtr: firibgarlik, manipulyatsiya va soxta axborot belgilarini tanish qobiliyati. Ikkinchi qatlam — irodaviy to‘xtam: shoshilinchlik va hissiy bosim ostida darhol harakat qilmasdan, to‘xtab o‘ylash va tekshirish odati. Bu qatlam D.Kanemanning ikkinchi tafakkur tizimini ongli ravishda ishga solishni anglatadi. Uchinchi qatlam — ijtimoiy tayanch: tahdidga duch kelganda yolg‘iz qolmasdan, ota-ona, o‘qituvchi yoki vakolatli organlarga murojaat qilish madaniyati. Bu qatlam ayniqsa kommunikativ-psixologik tahdidlarda hal qiluvchi ahamiyatga ega, chunki shantaj va bullying qurbonni yolg‘izlatish va sukut saqlashga majburlash orqali kuch oladi.

MUHOKAMA

Olingan natijalar kibertahdidlarga qarshi profilaktikaning an’anaviy usullarini qayta ko‘rib chiqishni taqozo etadi. Faqat qo‘rqitishga asoslangan ogohlantirishlar yoshlarda vaqtinchalik xavotir uyg‘otsa-da, barqaror himoya ko‘nikmalarini shakllantirmaydi. J.Roozenbek va S. van der Linden tadqiqotida manipulyatsiya usullari bilan o‘yin shaklida, zaiflashtirilgan namunalar orqali tanishgan ishtirokchilarning keyinchalik yolg‘on axborotga nisbatan ishonuvchanligi sezilarli pasaygani aniqlangan [10]. Bu “axborot emlash” yondashuvi kiberfiribgarlik profilaktikasiga ham qo‘llanilishi mumkin: yoshlarga firibgarlik ssenariylarini xavfsiz sharoitda “boshdan kechirish” imkonini beruvchi interaktiv mashg‘ulotlar ularda kognitiv filtr va irodaviy to‘xtamni amalda shakllantiradi. Xalqaro miqyosda keng tarqalgan “To‘xta. O‘yla. Ulan” tamoyiliga asoslangan targ‘ibot kampaniyalari ham aynan shu mantiqqa tayanadi.

Muhokama talab qiladigan muhim axloqiy masala — mas’uliyatning taqsimlanishidir. Kibermadaniyatni shaxsning himoya resursi sifatida ko‘rish jabrlanuvchini aybdor qilishga olib kelmasligi lozim. Agar firibgarlik qurboni bo‘lgan yosh atrofdagilar tomonidan “ehtiyotsiz” deb qoralansa, u keyingi safar sodir bo‘lgan holat haqida xabar berishdan uyaladi va bu jinoyatchilarning jazosiz qolishiga sabab bo‘ladi. Shu bois ichki ishlar organlari, ta’lim muassasalari va oilada jabrlanuvchiga hurmat va xayrixohlik bilan munosabatda bo‘lish, murojaat qilishni rag‘batlantiruvchi muhit yaratish kibermadaniyatning ijtimoiy tayanch qatlamini mustahkamlashning muhim shartidir. Shu bilan birga, xavfsizlik uchun mas’uliyat faqat foydalanuvchiga emas, balki davlat, bank tizimi va raqamli platformalarga ham tegishli ekanini unutmaslik kerak.

Milliy kontekstda bu masala o‘ziga xos dialektik tus oladi. Xalqimizga xos andisha, or-nomus va “uyat” madaniyati yoshlarni axloqsiz onlayn xatti-harakatlardan tiyib turuvchi kuchli ma’naviy omildir. Biroq aynan shu qadriyatlardan shantajchilar ham foydalanishga urinadi: ular qurbonni “sharmanda bo‘lish” qo‘rquvi bilan sukut saqlashga majburlaydi. Shu sababli tarbiya jarayonida yoshlarga uyat jabrlanuvchiga emas, balki jinoyat sodir etgan shaxsga tegishli ekanini, yordam so‘rash esa zaiflik emas, balki mas’uliyat belgisi ekanini tushuntirish muhimdir. Bu yondashuv milliy qadriyatlarni kibermadaniyatning himoya resursiga aylantiradi.

Tadqiqot nazariy-tahliliy xarakterga ega bo‘lib, taklif etilgan tipologiya va “raqamli immunitet” modelining samaradorligini yoshlar o‘rtasida o‘tkaziladigan so‘rovnomalar, tajriba-sinov mashg‘ulotlari va huquqbuzarliklar statistikasini tahlil qilish orqali empirik tekshirish keyingi tadqiqotlarning vazifasidir.

XULOSA

Tadqiqot natijalari kibertahdidlar asosan texnik tizimlarga emas, balki inson ongidagi zaifliklar — ishonuvchanlik, shoshilinchlik, qoʻrquv, ijtimoiy eʼtirofga ehtiyoj va moddiy manfaatga intilishga yoʻnaltirilganini koʻrsatdi. Ular iqtisodiy-firibgarlik, kommunikativ-psixologik, gʻoyaviy-manipulyativ va jinoiy jalb etish turlariga boʻlinadi. Xavf jamiyati sharoitida kibermadaniyat shaxsning asosiy himoya resursi boʻlib, u kognitiv filtr, irodaviy toʻxtam va ijtimoiy tayanchdan iborat “raqamli immunitet” sifatida namoyon boʻladi.

Shu asosda quyidagi takliflar ilgari suriladi: birinchidan, ichki ishlar organlari va taʼlim muassasalari hamkorligida firibgarlik ssenariylarini xavfsiz sharoitda mashq qilishga asoslangan interaktiv profilaktika dasturlarini ishlab chiqish; ikkinchidan, yoshlar uchun kibertahdidlar haqida xabar berishning qulay, maxfiy va jabrlanuvchini qoralamaydigan kanallarini kengaytirish; uchinchidan, yoshlar orasidan “kiber-volontyorlar” tarmogʻini shakllantirib, tengdoshlar oʻrtasida profilaktika ishlarini olib borish; toʻrtinchidan, bank kartasini boshqalarga berish va onlayn “oson daromad” takliflarining huquqiy oqibatlarini haqida yoshlarning huquqiy ongini oshirishga qaratilgan targʻibot ishlarini kuchaytirish.

Foydalanilgan adabiyotlar:

1. Oʻzbekiston Respublikasining “Kiberxavfsizlik toʻgʻrisida”gi Qonuni. 2022-yil 15-aprel.
2. Oʻzbekiston Respublikasi Prezidentining ““Raqamli Oʻzbekiston – 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari toʻgʻrisida”gi PF-6079-son Farmoni. 2020-yil 5-oktabr.
3. Oʻzbekiston Respublikasining “Bolalarni ularning sogʻligʻiga zarar yetkazuvchi axborotdan himoya qilish toʻgʻrisida”gi Qonuni. 2017-yil 8-sentabr.
4. Mirziyoyev Sh.M. Yangi Oʻzbekiston strategiyasi. – Toshkent: Oʻzbekiston, 2021.
5. Beck U. Risk Society: Towards a New Modernity. – London: Sage, 1992.
6. Kahneman D. Thinking, Fast and Slow. – New York: Farrar, Straus and Giroux, 2011.
7. Cialdini R.B. Influence: The Psychology of Persuasion. Rev. ed. – New York: Harper Business, 2006.
8. Suler J. The Online Disinhibition Effect // CyberPsychology & Behavior. – 2004. – Vol. 7, No. 3. – P. 321–326.
9. Kowalski R.M., Giumetti G.W., Schroeder A.N., Lattanner M.R. Bullying in the Digital Age: A Critical Review and Meta-Analysis of Cyberbullying Research Among Youth // Psychological Bulletin. – 2014. – Vol. 140, No. 4. – P. 1073–1137.
10. Roozenbeek J., van der Linden S. Fake News Game Confers Psychological Resistance Against Online Misinformation // Palgrave Communications. – 2019. – Vol. 5. – Article 65.