KIBER MAKONDA SHAXS, JAMIYAT VA DAVLAT XAVFSIZLIGI MUAMMOLARI

Sirojidinov Elyor Turg‘unpulat o‘g‘li
Namangan davlat universiteti tadqiqotchisi

DOI: https://doi.org/10.5281/zenodo.22765184

Annotatsiya*: Mazkur maqolada kiber makonning ontologik tabiati hamda unda shaxs, jamiyat va davlat xavfsizligi darajalari o‘rtasida yuzaga keladigan ko‘p qatlamli ziddiyatlar ijtimoiy-falsafiy metodologiya doirasida tadqiq etiladi. Muallif kiber makonni texnologik infratuzilmaning oddiy hosilasi sifatida emas, balki inson mavjudligining yangi ontologik qatlami — infosfera sifatida talqin qiladi va unda xavfsizlik muammosi klassik territorial paradigma vositalari bilan hal etilishi mumkin emasligini asoslaydi. Tadqiqotda raqamli identiklikning parchalanishi, ijtimoiy ishonch kapitalining yemirilishi, axborot suvereniteti chegaralarining noaniqlashuvi hamda deterritorializatsiyalashgan tahdid sub’ektlarining paydo bo‘lishi kiber xavfsizlikning asosiy strukturaviy determinantlari sifatida ko‘rsatib beriladi. Shuningdek, sekyuritizatsiya nazariyasi, infosfera etikasi va ishonch falsafasi negizida kiber xavfsizlikning uch tayanchli integrativ modeli taklif etiladi. Tahlil natijalari shuni ko‘rsatadiki, kiber makonda shaxs erkinligi, jamiyat barqarorligi va davlat suvereniteti o‘zaro raqobatlashuvchi qadriyatlar emas, balki bir-birini taqozo etuvchi, biroq muvozanatlashtirilishi zarur bo‘lgan konstitutiv jihatlardir.*

Kalit so‘zlar: *kiber makon, infosfera, axborot xavfsizligi, raqamli identiklik, ijtimoiy ishonch, axborot suvereniteti, sekyuritizatsiya, kiber tahdid, raqamli nazorat, virtual ijtimoiylashuv, axborot etikasi, kiber urush, raqamli mas’uliyat, texnologik determinizm, ijtimoiy-falsafiy tahlil.*

Abstract: *This article examines the ontological nature of cyberspace and the multilayered contradictions that arise between the levels of individual, societal, and state security within it through the framework of socio-philosophical methodology.*

The author interprets cyberspace not as a mere derivative of technological infrastructure, but as a new ontological layer of human existence — the infosphere — and substantiates that the security problem within it cannot be addressed solely through the means of the classical territorial paradigm. The study identifies the fragmentation of digital identity, the erosion of social trust capital, the ambiguity of the boundaries of information sovereignty, and the emergence of deterritorialized threat actors as the key structural determinants of cybersecurity. Furthermore, based on securitization theory, the ethics of the infosphere, and the philosophy of trust, an integrative three-pillar model of cybersecurity is proposed. The results of the analysis demonstrate that individual freedom, societal stability, and state sovereignty in cyberspace are not competing values, but rather constitutive dimensions that mutually condition one another while requiring an appropriate balance.

Keywords: *cyberspace, infosphere, information security, digital identity, social trust, information sovereignty, securitization, cyber threat, digital surveillance, virtual socialization, information ethics, cyber warfare, digital responsibility, technological determinism, socio-philosophical analysis.*

Аннотация: *В данной статье в рамках социально-философской методологии исследуются онтологическая природа киберпространства и многоуровневые противоречия, возникающие между уровнями безопасности личности, общества и государства в данной среде. Автор рассматривает киберпространство не как простое производное технологической инфраструктуры, а как новый онтологический слой человеческого бытия — инфосферу, и обосновывает невозможность решения проблемы безопасности в ней исключительно средствами классической территориальной парадигмы. В исследовании фрагментация цифровой идентичности, разрушение социального капитала доверия, неопределённость границ информационного суверенитета, а также появление детерриториализированных субъектов угроз рассматриваются в качестве*

основных структурных детерминант кибербезопасности. Кроме того, на основе теории секьюритизации, этики инфосферы и философии доверия предлагается интегративная трёхопорная модель кибербезопасности. Результаты анализа показывают, что свобода личности, стабильность общества и государственный суверенитет в киберпространстве не являются конкурирующими ценностями, а представляют собой конститутивные аспекты, взаимно обусловливающие друг друга, но требующие необходимого баланса.

Ключевые слова: *киберпространство, инфосфера, информационная безопасность, цифровая идентичность, социальное доверие, информационный суверенитет, секьюритизация, киберугроза, цифровой контроль, виртуальная социализация, информационная этика, кибервойна, цифровая ответственность, технологический детерминизм, социально-философский анализ.*

KIRISH

Kiber makonning paydo bo‘lishi va jadal kengayishi XX asr oxiri — XXI asr boshidagi eng chuqur sivilizatsion o‘zgarishlardan biri bo‘lib, u nafaqat kommunikatsiya vositalarini, balki insonning mavjud bo‘lish usulini, ijtimoiy tartibning tuzilishini hamda davlatning o‘z hokimiyatini amalga oshirish mexanizmlarini tubdan qayta shakllantirdi. An’anaviy xavfsizlik nazariyalari uch asr davomida xavfsizlikni territorial chegaralar, moddiy resurslar va harbiy-siyosiy kuch balansi kategoriyalari orqali talqin qilib keldi. Biroq kiber makon bu konseptual apparatni ishdan chiqardi: bu yerda chegara geografik emas, protokol darajasida o‘rnatiladi; tahdid manbai davlat bo‘lishi ham, o‘n olti yoshli o‘smir bo‘lishi ham mumkin; zarar esa bir necha millisekundda qit’alar osha tarqaladi. Shu bois kiber makonda xavfsizlik muammosi texnik-muhandislik masalasi doirasidan chiqib, mustaqil ijtimoiy-falsafiy tadqiqot predmeti maqomiga ko‘tarildi. Muammoning falsafiy o‘tkirligi uning ontologik asosidan kelib chiqadi. L. Floridi taklif etgan infosfera konsepsiyasiga ko‘ra, zamonaviy inson «onlayn» va «oflayn»

holatlar o‘rtasida qat’iy chegara mavjud bo‘lmagan onlife muhitida yashaydi. Raqamli ma’lumot bu yerda voqelikning aksi emas, balki voqelikning o‘zini tashkil etuvchi unsurga aylanadi. Bunday ontologik siljish xavfsizlik tushunchasining predmetini ham o‘zgartiradi: himoya qilinadigan obyekt endi faqat jismoniy tana yoki moddiy mulk emas, balki shaxsning axborot proyeksiyasi — uning raqamli izi, obro‘si, xulq-atvor profili va qaror qabul qilish avtonomiyasidir. Aynan shu sababli kiber makondagi tajovuz ko‘pincha jismoniy zo‘ravonliksiz amalga oshiriladi, biroq uning ekzistensial oqibatlari an’anaviy zo‘ravonlikdan kam bo‘lmasligi mumkin. Tadqiqot muammosining ikkinchi qatlami xavfsizlik sub’ektlarining ko‘pligi va ularning manfaatlari o‘rtasidagi ziddiyat bilan bog‘liq. Klassik xavfsizlik paradigmasida davlat yagona va ustuvor referent obyekt hisoblangan. Kopengagen maktabi vakillari B. Buzan, O. Vever va Ya. de Vilde ishlab chiqqan sekyuritizatsiya nazariyasi bu monopoliyani buzib, xavfsizlikning harbiy, siyosiy, iqtisodiy, ijtimoiy va ekologik sektorlarini ajratdi hamda xavfsizlik obyekti sifatida shaxs va jamiyat guruhlarini ham e’tirof etdi. Kiber makon sharoitida mazkur ko‘p darajalilik yanada murakkablashadi, chunki bu yerda uch daraja — shaxs, jamiyat va davlat — bir xil texnologik infratuzilmadan foydalanadi. Natijada bir darajadagi xavfsizlikni kuchaytirish ko‘pincha boshqa darajadagi xavfsizlikning pasayishi hisobiga amalga oshadi. Davlatning kiber nazorat imkoniyatlarini kengaytirishi milliy xavfsizlikni mustahkamlashi mumkin, biroq ayni paytda shaxsiy hayot daxlsizligini toraytiradi; individual anonimlikni mutlaqlashtirish esa jinoiy faoliyat uchun himoyalangan makon yaratadi. Ushbu antinomiya kiber xavfsizlik falsafasining markaziy muammosini tashkil etadi. Zamonaviy kiber tahdidlar tipologiyasini tahlil qilish ularning gibrid tabiatini oshkor etadi. Bugungi tajovuz kamdan kam hollarda sof texnik xarakterga ega bo‘ladi; u odatda texnologik vosita, psixologik ta’sir va ijtimoiy manipulyatsiyaning uyg‘unlashuvi sifatida namoyon bo‘ladi. Kritik infratuzilmaga qaratilgan hujumlar energetika, transport va sog‘liqni saqlash tizimlarining uzluksizligini xavf ostiga qo‘yadi; sun’iy intellekt vositalarida generatsiya qilinadigan soxta audio va video materiallar esa haqiqat va soxtalik

o‘rtasidagi chegarani idrok etish qobiliyatining o‘ziga putur yetkazadi. Falsafiy jihatdan bu holat epistemologik asoslarning inqiroziga olib keladi: agar ko‘rish va eshitish orqali olingan dalil ishonchli bo‘lmasa, jamoaviy voqelik tasavvurini shakllantiruvchi mexanizm ishdan chiqadi. Shu sababli zamonaviy kiber xavfsizlik nazariyasi ma’lumotning maxfiyligi, yaxlitligi va foydalanuvchanligi kabi klassik uchlikdan tashqariga chiqib, ishonchlilik va tasdiqlanuvchanlik kategoriyalarini ham qamrab olishi lozim. Aynan shu kengayish muammoni texnik fanlar doirasidan falsafiy tahlil maydoniga olib chiqadi.

Shaxs darajasida asosiy tahdid raqamli identiklikning zaifligi va parchalanishi bilan bog‘liq. Zamonaviy foydalanuvchi o‘z haqidagi ma’lumotlar ustidan real nazoratni yo‘qotgan holda, ko‘plab platformalarda tarqoq raqamli profillarga ega bo‘ladi. H. Nissenbaum ishlab chiqqan kontekstual yaxlitlik konsepsiyasi shaxsiy hayot daxlsizligining buzilishini ma’lumotning oshkor etilishi bilan emas, balki uning bir ijtimoiy kontekstdan boshqasiga norma buzilgan holda ko‘chirilishi bilan izohlaydi. Tibbiy ma’lumotning sug‘urta kompaniyasiga, xarid tarixining kredit skoringiga o‘tishi — bu aynan kontekstual normalarning buzilishidir. S. Zuboff esa nazorat kapitalizmi konsepsiyasi doirasida inson tajribasining bepul xomashyoga aylantirilishi va xulq-atvorni oldindan aytish hamda unga ta’sir ko‘rsatish mahsulotlarining shakllanishini tahlil qiladi. Bunday sharoitda shaxs xavfsizligi ma’lumotlarni himoya qilish masalasidan avtonomiyani saqlab qolish masalasiga aylanadi. Jamiyat darajasidagi tahdidlar ijtimoiy ishonch kapitalining yemirilishida namoyon bo‘ladi. M. Kastels asoslagan tarmoq jamiyati nazariyasiga ko‘ra, raqamli tarmoqlar ijtimoiy tuzilmaning yangi morfologiyasini yaratadi va hokimiyat oqimlar ustidan nazorat orqali amalga oshiriladi. Ushbu morfologiya kommunikatsiya imkoniyatlarini misli ko‘rilmagan darajada kengaytirish bilan birga, jamoatchilik fikrini manipulyatsiya qilishning yangi vositalarini ham vujudga keltiradi. Dezinformatsiya, algoritmik qutblanish, yolg‘on kontentni sun’iy intellekt yordamida generatsiya qilish jamiyatning umumiy voqelik tasavvurini parchalaydi. Falsafiy nuqtai nazardan bu epistemologik inqirozdir: jamiyat a’zolari faktlar

bo‘yicha emas, balki faktlarni aniqlash mezonlari bo‘yicha kelisha olmay qoladilar. Ishonchsizlik muhiti esa har qanday jamoaviy harakatning, jumladan xavfsizlikni ta’minlash bo‘yicha jamoaviy say’-harakatlarning ham asosini emiradi. Davlat darajasida muammo suverenitet kategoriyasining transformatsiyasi bilan bog‘liq. Vestfal tizimida suverenitet aniq belgilangan hudud ustidan oliy hokimiyat sifatida tushunilgan. Kiber makonda esa infratuzilma transmilliy korporatsiyalarga tegishli, ma’lumotlar bir necha yurisdiksiyada saqlanadi, hujum manbaini ishonchli aniqlash (atribusiya muammosi) ko‘pincha imkonsiz bo‘ladi. J. Nay kiber hokimiyat tahlilida hokimiyat resurslarining davlatdan nodavlat aktorlarga qisman diffuziyasini qayd etadi. T. Rid esa kiber hujumlarning aksariyati urush emas, balki josuslik, sabotaj va subversiyaning raqamli ko‘rinishi ekanligini asoslab, tahdidlarni kontseptual jihatdan farqlash zaruratini ko‘rsatadi. Bu esa davlat siyosatida mutanosiblik tamoyilini saqlash muammosini keltirib chiqaradi: haddan tashqari sekyuritizatsiya jamiyatni harbiylashtirilgan raqamli nazorat rejimiga olib kelishi mumkin. Muammoning mahalliy konteksti ham alohida ahamiyat kasb etadi. O‘zbekistonda amalga oshirilayotgan raqamli transformatsiya siyosati davlat xizmatlarini raqamlashtirish, elektron hukumat tizimini rivojlantirish va axborot infratuzilmasini modernizatsiya qilishni nazarda tutadi. Bunday jarayonlar samaradorlikni oshirish bilan birga, tizimning zaiflik nuqtalarini ham ko‘paytiradi. Aholining raqamli savodxonligi va axborot xavfsizligi madaniyati darajasi esa texnologik rivojlanish sur’atidan ortda qolmoqda. Shu sababli milliy kiber xavfsizlik strategiyasi faqat texnik himoya choralariga emas, balki ta’lim, huquqiy madaniyat va axloqiy mas’uliyatni shakllantirishga tayanishi lozim. Uzluksiz ta’lim tizimi orqali yoshlarning ma’naviy-falsafiy dunyoqarashini yuksaltirish masalasi bu yerda bevosita xavfsizlik masalasi sifatida namoyon bo‘ladi. Mazkur maqolaning maqsadi kiber makonda shaxs, jamiyat va davlat xavfsizligi o‘rtasidagi munosabatlarning ijtimoiy-falsafiy tabiatini ochib berish, ularning o‘zaro ziddiyatli va ayni paytda bir-birini taqozo etuvchi xususiyatini asoslash hamda muvozanatlashtirilgan kiber xavfsizlik modelining konseptual asoslarini ishlab chiqishdan iborat. Tadqiqot

metodologik jihatdan tizimli yondashuv, germenevtik tahlil, qiyosiy-falsafiy metod va ijtimoiy konstruktivizm tamoyillariga tayanadi. Ilmiy yangilik kiber xavfsizlikning uch darajasini yagona integrativ model doirasida birlashtirish hamda erkinlik, ishonch va mas’uliyat kategoriyalarini ushbu modelning tayanch o‘qlari sifatida asoslashdan iborat. Tadqiqot vazifalari quyidagilardan tashkil topadi: kiber makonning ontologik maqomini aniqlash; xavfsizlik sub’ektlari o‘rtasidagi manfaatlar ziddiyatining tabiatini ochib berish; ushbu ziddiyatni boshqarish tamoyillarini asoslash hamda milliy sharoitda madaniy-ma’rifiy chora-tadbirlarning ustuvorligini ko‘rsatishdan iborat.

Kiber makonni falsafiy jihatdan tavsiflashda ikki ekstremal yondashuvdan qochish zarur. Texnologik determinizm uni inson irodasidan mustaqil ravishda ijtimoiy tartibni belgilovchi kuch sifatida talqin qiladi; ijtimoiy konstruktivizmning radikal shakli esa uni butunlay ijtimoiy munosabatlar hosilasiga reduksiya qiladi. Haqiqat oraliqda joylashgan: kiber makon inson tomonidan yaratilgan, biroq yaratuvchisiga nisbatan nisbiy avtonomiyaga ega bo‘lgan sun’iy ontologik qatlamdir. Uning arxitekturasi — protokollar, algoritmlar, platforma qoidalari — L. Lessig ta’biri bilan aytganda, o‘ziga xos «kod-qonun» sifatida amal qiladi va foydalanuvchi xulqini huquqiy normalardan ko‘ra samaraliroq boshqaradi.

Ushbu ontologik xususiyat xavfsizlik sub’ektini aniqlash muammosini keltirib chiqaradi. An’anaviy paradigmada himoya qiluvchi va himoya qilinuvchi o‘rtasida aniq chegara mavjud edi. Kiber makonda esa foydalanuvchining o‘zi bir vaqtning o‘zida himoya obyekti, zaiflik manbai va potensial tahdid vektori bo‘lib chiqadi. Statistik ma’lumotlar muvaffaqiyatli hujumlarning katta qismi texnik zaifliklar emas, balki inson omili — ijtimoiy injiniring, e’tiborsizlik, past raqamli savodxonlik orqali amalga oshirilishini ko‘rsatadi. Demak, kiber xavfsizlikning o‘zagi texnologik emas, antropologik tabiatga ega. Uch darajadagi xavfsizlik manfaatlari o‘rtasidagi munosabat chiziqli emas. Shaxs darajasida ustuvor qadriyat — avtonomiya va shaxsiy hayot daxlsizligi; jamiyat darajasida — ishonch, hamjihatlik va kommunikativ barqarorlik; davlat darajasida — suverenitet,

infratuzilma yaxlitligi va boshqaruv qobiliyati. Mazkur qadriyatlar o‘zaro zid emas, biroq ularni bir vaqtning o‘zida maksimallashtirish mumkin emas: biri uchun optimal yechim ikkinchisi uchun risk hosil qiladi. Antinomiyaning klassik ko‘rinishi «xavfsizlik — erkinlik» dilemmasidir. U. Bek asoslagan risk jamiyati nazariyasi bu dilemmani yangi kontekstda tushuntiradi: xavf-xatarlarni boshqarishga yo‘naltirilgan institutlar o‘zlari yangi xavflar manbaiga aylanishi mumkin. Ommaviy raqamli nazorat tizimlari aynan shunday paradoksni yuzaga keltiradi — ular jinoyatchilikka qarshi kurash samaradorligini oshirsa-da, fuqarolarning davlatga bo‘lgan ishonchini pasaytirishi va sovuqqonlik effektini keltirib chiqarishi mumkin. Antinomiyani bartaraf etishning yagona yo‘li qadriyatlardan birini qurbon qilish emas, balki mutanosiblik tamoyili asosida institutsional muvozanat mexanizmini yaratishdir. Bunda har qanday cheklov qonuniy asosga ega bo‘lishi, aniq maqsad bilan chegaralanishi, mustaqil nazorat ostida bo‘lishi va vaqt jihatidan cheklangan bo‘lishi talab etiladi.

O‘tkazilgan tahlil asosida kiber xavfsizlikning uch tayanchli falsafiy modelini taklif etish mumkin. Birinchi tayanch — erkinlikning himoyalanishi: shaxsning raqamli avtonomiyasi, ma’lumotlari ustidan nazorat huquqi va algoritmik qarorlarga nisbatan e’tiroz bildirish imkoniyati. Ikkinchi tayanch — ishonchning institutsionallashuvi: shaffof qoidalar, tekshiriluvchi algoritmlar va mustaqil nazorat organlari orqali kommunikativ muhitning ishonchliligini ta’minlash. Uchinchi tayanch — mas’uliyatning taqsimlanishi: xavfsizlik faqat davlat organlarining vazifasi emas, balki platformalar, ta’lim muassasalari, oila va har bir foydalanuvchining birgalikdagi mas’uliyati sifatida tushunilishi. Ushbu tayanchlar bir-birini almashtira olmaydi. Erkinliksiz ishonch itoatkorlikka, ishonchsiz mas’uliyat rasmiyatchilikka, mas’uliyatsiz erkinlik esa anarxiyaga aylanadi. Modelning amaliy joriy etilishi uzluksiz ta’lim tizimi orqali raqamli-axloqiy kompetensiyani shakllantirishni talab qiladi, chunki kiber makonda xavfsizlikning eng ishonchli kafolati — bu ongli, tanqidiy fikrlaydigan va mas’uliyatni his qiladigan foydalanuvchidir.

XULOSA

O‘tkazilgan ijtimoiy-falsafiy tahlil kiber makonda xavfsizlik muammosining an’anaviy territorial paradigma doirasida hal etilishi mumkin emasligini ko‘rsatdi. Birinchidan, kiber makon texnologik vositalar majmui emas, balki inson mavjudligining yangi ontologik qatlami bo‘lib, unda himoya obyekti jismoniy tana yoki moddiy mulk emas, shaxsning axborot proyeksiyasi va qaror qabul qilish avtonomiyasidir. Ikkinchidan, shaxs, jamiyat va davlat xavfsizligi darajalari yagona texnologik infratuzilmada birlashgani bois ular o‘rtasida barqaror antinomiya mavjud: bir darajadagi himoyani mutlaqlashtirish boshqa darajadagi zaiflikni kuchaytiradi. Mazkur antinomiya yo‘q qilinmaydi, balki mutanosiblik tamoyili asosida boshqariladi. Uchinchidan, kiber tahdidlarning asosiy manbai texnik zaifliklar emas, inson omili ekanligi kiber xavfsizlikning antropologik tabiatini tasdiqlaydi. Demak, eng samarali investitsiya — dasturiy himoya vositalariga emas, foydalanuvchining ma’naviy-intellektual salohiyatiga qilinadigan investitsiyadir. To‘rtinchidan, taklif etilgan uch tayanchli model — erkinlikni himoyalash, ishonchni institutsionallashtirish va mas’uliyatni taqsimlash — kiber xavfsizlikni yaxlit tizim sifatida tashkil etishning konseptual asosini beradi. Ushbu tayanchlar o‘zaro almashinuvchi emas, balki bir-birini taqozo etuvchi elementlardir. Beshinchidan, O‘zbekistonda amalga oshirilayotgan raqamli transformatsiya siyosati kiber xavfsizlik madaniyatini shakllantirish uchun qulay institutsional asos yaratmoqda. Uning to‘liq samarasi esa uzluksiz ta’lim tizimi orqali yoshlarda tanqidiy fikrlash, axborot gigiyenasi va raqamli mas’uliyat ko‘nikmalarining qaror topishiga bog‘liq. Kiber makonda jamiyat o‘z a’zolarining ongliligiga qanchalik ishona olsa, u shunchalik himoyalangan bo‘ladi.

Foydalanilgan adabiyotlar

1. Ergashbaev S. O‘zbekiston sharoitida uzluksiz ta’lim tizimi orqali yoshlarning ma’naviy dunyoqarashini rivojlantirish // Объединяя студентов: международные исследования и сотрудничество между дисциплинами. — 2025. — Т. 1, № 1. — С. 314—316.

2. Castells M. The Rise of the Network Society. — Oxford: Blackwell Publishers, 1996. — 556 p.

3. Buzan B., Wæver O., de Wilde J. Security: A New Framework for Analysis. — Boulder, CO: Lynne Rienner Publishers, 1998. — 239 p.

4. Ergashbayev S. Uzluksiz ta’lim tashkil etish orqali yoshlarning ma’naviy-falsafiy dunyoqarashini yuksaltirish // Bulletin of Contemporary Researches: Multidisciplinary. — 2025. — Vol. 1, № 1. — P. 10—13.

5. Nissenbaum H. Privacy in Context: Technology, Policy, and the Integrity of Social Life. — Stanford, CA: Stanford University Press, 2009. — 288 p.

6. Floridi L. The Fourth Revolution: How the Infosphere is Reshaping Human Reality. — Oxford: Oxford University Press, 2014. — 248 p.

7. Mirzaolimjon og‘li M.M., Shohbozbek E. Yangi O‘zbekistonning ta’lim siyosati va universitetlarning yangi modellari // Pedagogik islohotlar va ularning yechimlari. — 2025. — Vol. 16, № 01. — B. 325—328.

8. Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. — New York: PublicAffairs, 2019. — 704 p.

9. Nye J.S. Cyber Power. — Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010. — 24 p.

10. Rid T. Cyber War Will Not Take Place // Journal of Strategic Studies. — 2012. — Vol. 35, № 1. — P. 5—32.