O‘ZBEKISTON MILLIY UNIVERSITETI XABARLARI, 2026, [7]
ISSN 2181-7324(Print)

IJTIMOIY FANLAR
http://journals.nuu.uz
ISSN 3093-8996(Onlayn)

UDK:004.056(470+571)

***Jaxongir ALIYEV,***
*Toshkent davlat sharqshunoslik universiteti tayanch doktoranti*
*Email: aliyevjahongir2330@gmail.com*

*DSc, dotsent M.Tursunov taqrizi asosida*

## ROSSIYADA AXBOROT XAVFSIZLIGINI TA’MINLASH TAJRIBASI

Annotatsiya

Mazkur maqolada Rossiya Federatsiyasida axborot xavfsizligini ta’minlash siyosatining shakllanish bosqichlari, uning asosiy ustuvor yo‘nalishlari, tashqi propaganda va dezinformatsiyaga qarshi qo‘llanilayotgan huquqiy, texnologik hamda institutsional mexanizmlar tahlil qilinadi. Shuningdek, ushbu tajribaning rus va g‘arb olimlari tomonidan talqin etilishi yoritiladi. Tadqiqot natijalari Rossiyada axborot xavfsizligi tor ma’nodagi kiberxavfsizlik emas, balki siyosiy va axborot suvereniteti, jamiyat ongini himoya qilish, tarixiy-madaniy identitetni saqlash bilan bog‘liq keng xavfsizlik kategoriyasi sifatida tushunilishini ko‘rsatadi.

**Kalit so‘zlar:** Rossiya, axborot xavfsizligi, axborot suvereniteti, dezinformatsiya, propaganda, suveren internet, axborot-psixologik ta’sir.

## RUSSIA’S EXPERIENCE IN ENSURING INFORMATION SECURITY

Annotation

This article analyzes the stages in the formation of the information security policy of the Russian Federation, its main priority areas, as well as the legal, technological, and institutional mechanisms employed to counter external propaganda and disinformation. It also examines how this experience has been interpreted by Russian and Western scholars. The findings demonstrate that, in Russia, information security is understood not merely as cybersecurity in the narrow sense, but as a broader security category associated with political and information sovereignty, the protection of public consciousness, and the preservation of historical and cultural identity.

**Keywords:** Russia, information security, information sovereignty, disinformation, propaganda, sovereign internet, information-psychological influence.

## ОПЫТ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ

Аннотация

В данной статье анализируются этапы становления политики Российской Федерации в сфере обеспечения информационной безопасности, её основные приоритетные направления, а также правовые, технологические и институциональные механизмы, применяемые для противодействия внешней пропаганде и дезинформации. Кроме того, рассматривается интерпретация данного опыта российскими и западными исследователями. Результаты исследования показывают, что в России информационная безопасность понимается не только как кибербезопасность в узком смысле, но и как более широкая категория безопасности, связанная с политическим и информационным суверенитетом, защитой общественного сознания, а также сохранением историко-культурной идентичности.

**Ключевые слова:** Россия, информационная безопасность, информационный суверенитет, дезинформация, пропаганда, суверенный интернет, информационно-психологическое воздействие.

**Kirish.** Zamonaviy Zamonaviy xalqaro munosabatlarda axborot makoni davlat xavfsizligining muhim o‘lchamlaridan biriga aylandi. Endilikda davlat barqarorligi faqat harbiy, iqtisodiy yoki diplomatik salohiyat bilan emas, balki raqamli infratuzilmani himoya qilish, axborot oqimlarini boshqarish va tashqi axboriy bosimlarni cheklash bilan ham belgilanadi. Shu jihatdan Rossiya Federatsiyasi tajribasi alohida e’tiborga loyiq, chunki bu davlat axborot xavfsizligini faqat texnik yoki kiber masala sifatida emas, balki siyosiy suverenitet, jamiyat barqarorligi va ma’naviy qadriyatlar bilan bog‘liq keng xavfsizlik sohasi sifatida talqin etadi.

Rossiyada bu yondashuv 2000-yildan boshlab aniq institutsional shakl oldi. 2000-yilgi Axborot xavfsizligi doktrinasi ushbu yo‘nalishni milliy xavfsizlik siyosatining alohida tarkibiy qismi sifatida mustahkamladi [1]. 2016-yilgi yangi doktrina esa xorijiy axboriy ta’sir, ijtimoiy-siyosiy barqarorlikka zarar yetkazuvchi informatsion bosim va madaniy qadriyatlarga putur yetkazuvchi kommunikativ amaliyotlarni tahdid sifatida belgiladi [2]. 2017-yildagi Axborot jamiyatini rivojlantirish strategiyasi esa axborot xavfsizligini raqamli iqtisodiyot va milliy texnologik salohiyat bilan bog‘ladi [3].

Mazkur mavzuning dolzarbligi shundaki, Rossiya tajribasi axborot xavfsizligi bilan axborot nazoratining o‘zaro tutashuvini ko‘rsatadi. Bir tomondan, Rossiya o‘z siyosatini tashqi propaganda, dezinformatsiya va axborot-psixologik ta’sirga qarshi mudofaa sifatida asoslaydi. Ikkinchi tomondan, xalqaro kuzatuvlar bunday choralar ichki axborot maydonini markazlashtirish va platformalar ustidan nazoratni kuchaytirish bilan ham bog‘liq ekanini ko‘rsatadi [4]. Shu bois Rossiya tajribasini murakkab siyosiy-amaliy hodisa sifatida tahlil qilish zarur [5].

Mazkur maqolaning maqsadi Rossiyada axborot xavfsizligini ta’minlash siyosatining shakllanishi, ustuvor yo‘nalishlari va dezinformatsiyaga qarshi kurash vositalarini yoritishdan iborat. Maqolaning ilmiy yangiligi shundaki, unda Rossiya tajribasi texnik-infratuzilmaviy himoya, axborot-psixologik himoya va siyosiy-suveren boshqaruvdan iborat uch qatlamli model asosida tushuntiriladi.

**Adabiyotlar sharhi.** Rossiyada axborot xavfsizligi bo‘yicha mavjud adabiyotlar bir xil yondashuvga ega emas.

Ularni umumiy tarzda to‘rt yo‘nalishga ajratish mumkin. Birinchi yo‘nalishni rasmiy-doktrinal hujjatlar tashkil etadi. Ikkinchisi rus olimlarining geosiyosiy va axborot-psixologik qarashlari bilan bog‘liq. Uchinchi yo‘nalishda g‘arb tadqiqotchilarining strategik va konseptual tahlillari turadi. To‘rtinchi yo‘nalish esa internet boshqaruvi hamda raqamli nazoratga doir empirik ishlarni qamrab oladi. Ana shu qatlamlarni birgalikda ko‘rib chiqish Rossiya modelining ichki mantig‘ini yaxshiroq tushunishga yordam beradi.

Rasmiy hujjatlar Rossiyada axborot xavfsizligi masalasining qanday talqin qilinishini aniq ko‘rsatadi. 2000-yilgi Axborot xavfsizligi doktrinasi bu tushunchani shaxs, jamiyat va davlat manfaatlarini axborot sohasida himoya qilish bilan bog‘laydi. 2016-yilgi doktrina esa tahdidlar doirasini kengaytirib, xorijiy informatsion ta’sir, milliy qadriyatlarni yemirish, jamiyat ongiga buzg‘unchi ta’sir ko‘rsatish hamda ijtimoiy barqarorlikka putur yetkazish kabi omillarni ham xavf sifatida qayd etadi. 2017-yilgi strategiyada esa ushbu yondashuv texnologik mustaqillik, milliy dasturiy mahsulotlar va raqamli iqtisodiyot bilan bog‘lanadi. Shu bois rasmiy manbalar Rossiyada axborot xavfsizligi tor ma’nodagi “cybersecurity” emas, balki ancha keng va mafkuraviy mazmunga ega ekanini ko‘rsatadi.

Rus olimlari orasida Andrey Manoilo alohida e’tiborga loyiq. U axborot urushi texnologiyalari va psixologik operatsiyalarni xalqaro siyosatning real vositalaridan biri sifatida tahlil qiladi va axborot xavfsizligini axborot-psixologik ta’sir, manipulyativ texnologiyalar hamda siyosiy kommunikatsiya bilan bog‘laydi [6]. Krutskikh va Streltsov esa ko‘proq xalqaro axborot xavfsizligi konsepsiyasi doirasida ish olib boradi. Ularning qarashlarida axborot xavfsizligi davlatlarning suveren tengligi, xalqaro huquq va BMT me’yorlari bilan bog‘lanadi [7]. Umuman olganda, rus ilmiy maktabi bu masalaga ko‘proq davlat markazchi va suverenitetga yo‘naltirilgan nuqtai nazardan qaraydi.

G‘arb tadqiqotchilari esa Rossiya tajribasini boshqacharoq talqin qiladi. Keir Giles Rossiya axborot urushini bir martalik kampaniya emas, balki doimiy strategik faoliyat sifatida ko‘rsatadi [8]. Ofer Fridman Rossiya “hybrid warfare” va “information warfare” tushunchalarining g‘arbda ko‘pincha soddalashtirilgan holda talqin qilinishini tanqid qiladi va ularning asl strategik mazmuniga e’tibor qaratadi [9]. Katri Pynnöniemi esa Rossiya xavfsizlik tafakkurida axborot-psixologik urush mavzusi anchadan beri muhim o‘rin tutishini ko‘rsatadi va bu yondashuvning tarixiy ildizlari chuqur ekanini asoslaydi [10].

Empirik tadqiqotlar ham Rossiya modelini tushunishda muhim o‘rin tutadi. Mariëlle Wijermars internet nazorati, xususan Telegram’ni bloklash tajribasi misolida, bunday cheklovlar xavfsizlik, terrorizmga qarshi kurash va davlat manfaatlarini himoya qilish diskursi orqali qanday oqlanishini ko‘rsatadi [11]. Freedom House, DGAP va Carnegie kabi manbalar esa “suveren internet” siyosati davlatning internet ustidan nazoratini sezilarli darajada kuchaytirganini ta’kidlaydi [12]. Shunday qilib, empirik adabiyotlar Rossiya modelida huquqiy, texnik va diskursiv vositalar bir-biri bilan chambarchas bog‘liq ekanini ko‘rsatadi.

Umuman olganda, adabiyotlar sharhi ikki muhim xulosaga olib keladi. Birinchidan, rus mualliflari axborot xavfsizligini asosan tashqi tahdidlarga qarshi davlat va jamiyatni himoya qilish vositasi sifatida talqin qiladi. Ikkinchidan, g‘arb tadqiqotchilari ayni shu siyosatning ichki oqibatlari, ya’ni internet nazorati, kommunikativ maydonni markazlashtirish va siyosiy boshqaruvni kuchaytirishga ko‘proq urg‘u beradi [13]. Shu sabab Rossiya tajribasini faqat xavfsizlik modeli sifatida emas, balki axborot boshqaruvi modeli sifatida ham o‘rganish zarur.

**Metodologiya.** Maqolaning asosiy maqsadi Rossiyada axborot xavfsizligi qanday tarixiy-siyosiy mantiq asosida shakllangani, tashqi propaganda va dezinformatsiyaga qarshi qanday vositalar qo‘llanayotgani hamda bu jarayon ilmiy adabiyotlarda qanday talqin qilinayotganini aniqlashdan iborat bo‘ldi. Shu maqsadda normativ-huquqiy tahlil, tarixiy-genealogik yondashuv, qiyosiy adabiyot tahlili va diskursiv tahlil birgalikda qo‘llanildi. Bunday yondashuv Rossiya tajribasini rasmiy hujjatlar, ilmiy qarashlar va amaliy boshqaruv mexanizmlari o‘rtasidagi uzviy bog‘liqlikda ko‘rish imkonini berdi.

Normativ-huquqiy tahlilda Rossiyaning axborot xavfsizligiga oid uch asosiy hujjati tanlab olindi. Bular 2000-yilgi doktrina, 2016-yilgi yangilangan doktrina va 2017–2030-yillarga mo‘ljallangan strategiyadir. Mazkur hujjatlar Rossiya davlatining ushbu sohadagi rasmiy qarashlarini izchil aks ettirgani uchun asosiy manba sifatida olindi. Tahlilda axborot xavfsizligining ta’rifi, tahdidlar tasnifi va davlat javob choralarining yo‘nalishiga alohida e’tibor qaratildi.

Tarixiy-genealogik yondashuv Rossiya axborot xavfsizligi modelini birdan paydo bo‘lgan hodisa emas, balki uzoq davom etgan siyosiy va intellektual evolyutsiya mahsuli sifatida ko‘rib chiqishga xizmat qildi. Bu yerda 2000-yilgi doktrina boshlang‘ich institutsional bosqich, 2016-yilgi doktrina esa siyosiy va mafkuraviy jihatlari kuchaygan keyingi bosqich sifatida talqin qilindi. Pynnöniemi tomonidan axborot-psixologik urushning rus harbiy tafakkurida 1960-yillardan beri muhim mavzu bo‘lib kelgani haqidagi fikr ushbu yondashuv uchun muhim tayanch bo‘ldi [10].

Qiyosiy adabiyot tahlilida rus va g‘arb mualliflari alohida korpuslarga ajratildi. Diskursiv tahlilda esa “axborot xavfsizligi”, “tashqi ta’sir”, “suveren internet” va “axborot-psixologik ta’sir” kabi tushunchalarning siyosiy mazmuni ochib berildi [11]. Shu asosda Rossiya axborot xavfsizligi modeli texnik-infratuzilmaviy, axborot-psixologik va siyosiy-suveren qatlamlardan iborat degan ishchi gipoteza ilgari surildi.

**Tahlil va natijalar.** Tahlil natijalari shuni ko‘rsatadiki, Rossiyada axborot xavfsizligiga davlat darajasida tizimli yondashuv 2000-yilgi doktrina bilan aniq institutsional shakl oldi. Ushbu hujjatda axborot xavfsizligi davlat siyosatini belgilovchi rasmiy qarashlar tizimi sifatida ta’riflandi [1]. Aynan shu bosqichdan boshlab Rossiyada axborot sohasi shaxs, jamiyat va davlat manfaatlarini himoya qilish bilan bog‘liq alohida strategik yo‘nalish sifatida qarala boshlandi. Muhimi, bu yondashuv axborot xavfsizligini tor texnik masala sifatida emas, balki davlat boshqaruvi, milliy manfaat va siyosiy barqarorlik bilan chambarchas bog‘liq kengroq soha sifatida shakllantirdi.

Rossiya modelining keyingi muhim bosqichi 2016-yilgi yangilangan doktrina bilan bog‘liq. Ushbu hujjatda xorijiy davlatlar va tashkilotlarning Rossiyaga informatsion ta’siri, rus ommaviy axborot vositalariga nisbatan cheklovlar, jamiyatga destruktiv axborot ta’siri, tarixiy qadriyatlar hamda an’anaviy ma’naviy asoslarning yemirilishi, shuningdek ijtimoiy-siyosiy vaziyatni beqarorlashtirish xavfi alohida tahdid sifatida ko‘rsatildi [2]. Bu esa Rossiyada axborot xavfsizligi tushunchasi 2016-yildan boshlab yanada siyosiy va mafkuraviy mazmun kasb etganini anglatadi. Endilikda masala faqat tarmoq va resurslarni himoya qilish bilan cheklanmay, jamiyat ongini va ichki barqarorlikni saqlash bilan ham bog‘landi.

2017-yildagi Axborot jamiyatini rivojlantirish strategiyasi esa bu siyosatni texnologik rivojlanish bilan uyg‘unlashtirdi. Unda milliy raqamli iqtisodiyot, mahalliy dasturiy ta’minot, ishonchli infratuzilma va raqamli sohadagi milliy manfaatlarni ta’minlash xavfsizlik bilan birgalikda ko‘rib chiqildi [3]. Shu tariqa Rossiya modelida raqamli taraqqiyot va raqamli suverenitet bir-biridan ajratilmagan, balki o‘zaro bog‘liq strategik yo‘nalishlar sifatida talqin etiladi.

Amaliy mexanizmlar tahlili Rossiyada tashqi propaganda va dezinformatsiyaga qarshi kurash uch asosiy darajada olib

borilishini ko‘rsatadi. Birinchi daraja — huquqiy cheklovlardir. 2019-yilda qabul qilingan anti-fake-news qonunlari “ijtimoiy ahamiyatga ega ishonchsiz axborot” tarqatilishiga qarshi normativ asos yaratdi. Library of Congress sharhiga ko‘ra, bu normalar hayot, sog‘liq, mulk, jamoat tartibi yoki muhim infratuzilma faoliyatiga xavf tug‘dirishi mumkin bo‘lgan axborotga nisbatan tezkor choralar ko‘rish imkonini berdi [4]. Biroq bunday keng ta’rif davlat organlariga qaysi axborotni “ishonchsiz” deb topish masalasida katta talqin imkonini ham yaratdi.

Ikkinchi daraja texnologik va infratuzilmaviy boshqaruv bilan bog‘liq. 2019-yildagi “suveren internet” qonuni rasmiy jihatdan Rossiya internet segmentini tashqi xavflardan himoya qilishga qaratilgan bo‘lsa-da, mustaqil tahlillarda u davlatga internet ustidan markazlashgan boshqaruv tizimini yaratish, zarurat tug‘ilganda tarmoqni izolyatsiya qilish va trafik ustidan chuqurroq nazorat o‘rnatish imkonini berishi ta’kidlanadi. Freedom House ham bu qonun Rossiya segmentini global internetdan nisbatan mustaqil ishlashga tayyorlashga qaratilganini qayd etadi [12].

Uchinchi daraja esa narrativ va diskursiv kurashdir. Rossiya tashqi propaganda va dezinformatsiyaga qarshi faqat rad etish yoki faktlarni tekshirish bilan cheklanmaydi. U rasmiy narrativlarini mustahkamlash, davlatga yaqin kommunikatsiya kanallarini kuchaytirish va voqelikning siyosiy jihatdan maqbul talqinini keng tarqatish orqali ham javob beradi [8]. Shu sabab Rossiya tajribasini umumlashtirganda, uning uch qatlamli modeli yaqqol ko‘rinadi: texnik-infratuzilmaviy himoya, axborot-psixologik himoya va siyosiy-suveren boshqaruv. Ana shu uch qatlam birgalikda Rossiyada axborot xavfsizligi siyosatining asosiy mazmunini tashkil etadi.

**Muhokama.** Olingan natijalar shuni ko‘rsatadiki, Rossiya axborot xavfsizligi modelini faqat kiberxavfsizlik doirasida tushuntirish yetarli emas. Rossiya rasmiy hujjatlari va ekspert diskursida axborot xavfsizligi davlat suvereniteti, ijtimoiy barqarorlik, tarixiy xotira va jamoatchilik ongiga qaratilgan tashqi ta’sirlarni jilovlash bilan uzviy bog‘langan [1]. Shu sabab Rossiya modeli “cybersecurity”dan ko‘ra kengroq “information security” paradigmasiga tayanadi. Bu yondashuv texnik himoyani siyosiy va mafkuraviy mudofaa bilan birlashtiradi.

Aynan shu nuqtada rus va g‘arb yondashuvlari o‘rtasidagi asosiy farq yaqqol namoyon bo‘ladi. Rus mualliflari, xususan Manoilo hamda Krutskikh-Streltsov, axborot xavfsizligini asosan tashqi informatsion bosimga qarshi davlat va jamiyatni himoya qilish vositasi sifatida talqin qiladi [7]. G‘arb mualliflari esa bu choralarining ichki oqibatlariga e’tibor qaratadi. Masalan, Giles Rossiya modelini doimiy strategik qarama-qarshilik mahsuli sifatida tahlil qiladi [8], Fridman tushunchaviy siyosiylashuvni ko‘rsatadi [9], Wijermars esa internet boshqaruvi va cheklovlarning qanday legitimlashtirilishini ochib beradi [11]. Shu tariqa bir xil amaliyot turli nazariy yondashuvlarda turlicha talqin qilinadi.

Rossiya tajribasining eng bahsli jihati shundaki, unda “himoya” va “nazorat” o‘rtasidagi chegara torayadi. Anti-fake-news qonunlari, suveren internet siyosati va platformalar ustidan nazorat tashqi tahdidlarga javob sifatida taqdim etiladi, biroq amalda ular ichki axborot makonini markazlashtirish va siyosiy boshqaruvni kuchaytirishga ham xizmat qiladi [13]. Shu bois Rossiya modelini na faqat oqilona mudofaa tizimi, na faqat senzura mexanizmi sifatida biryoqlama baholash to‘g‘ri bo‘lmaydi. Pynnöniemi ta’kidlaganidek, axborot-psixologik urush Rossiya strategik tafakkurida uzoq tarixga ega [10], va aynan shu tarixiy fon davlatning axborot makoniga aralashuvini strategik zarurat sifatida asoslashga xizmat qiladi.

**Xulosa va takliflar.** Rossiyada axborot xavfsizligini ta’minlash siyosati 2000-yildan boshlab izchil institutsionallashib, 2016-yilgi doktrina va 2017-yilgi strategiya bilan yanada kengaydi. Tahlil shuni ko‘rsatdiki, Rossiya yondashuvida axborot xavfsizligi tor texnik kategoriya emas, balki siyosiy suverenitet, jamiyat barqarorligi, tarixiy xotira, ma’naviy qadriyatlar va informatsion makon ustidan nazorat bilan bog‘liq kompleks tushunchadir. Maqoladagi asosiy ilmiy xulosa shundan iboratki, Rossiya tajribasi uch qatlamli model asosida tushuntirilishi mumkin: texnik-infratuzilmaviy himoya, axborot-psixologik himoya va siyosiy-suveren boshqaruv. Bu model Rossiya siyosatini yaxlit tushunishga yordam beradi va uni faqat “kiberxavfsizlik” doirasida talqin qilishning cheklanganligini ko‘rsatadi.

Shuningdek, tahlil Rossiyada tashqi propaganda va dezinformatsiyaga qarshi kurash huquqiy, texnologik va diskursiv vositalarning uyg‘unlashuvi asosida olib borilishini ko‘rsatdi. Biroq ushbu vositalar ichki axborot maydonini qayta tartiblash, platformalar ustidan nazoratni kuchaytirish va muqobil kommunikatsiyani cheklash bilan ham tutashib ketadi. Shu sabab Rossiya tajribasi bir vaqtning o‘zida ham xavfsizlik siyosati, ham kommunikativ markazlashuv modeli sifatida o‘rganilishi lozim.

Kelgusida ushbu modelni boshqa davlatlar tajribasi bilan qiyosiy ravishda o‘rganish, ayniqsa axborot xavfsizligi va axborot nazorati o‘rtasidagi chegarani aniqlash, zamonaviy siyosatshunoslik va xalqaro munosabatlar tadqiqotlari uchun muhim ilmiy istiqbol bo‘lib qoladi.

**ADABIYOTLAR**


1. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 9 сентября 2000 г.
2. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.
3. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы. Указ Президента Российской Федерации от 9 мая 2017 г. № 203.
4. Initiatives to Counter Fake News in Selected Countries. Law Library of Congress, 2019.
5. Deciphering Russia’s “Sovereign Internet Law”. German Council on Foreign Relations (DGAP), 2020.
6. Манойло А.В. Информационные войны и психологические операции: руководство к действию. 2019.
7. Крутских А.В., Стрельцов А.А. Международная информационная безопасность / Международное право и проблема обеспечения международной информационной безопасности.
8. Giles, Keir. Handbook of Russian Information Warfare. NATO Defense College, 2016.
9. Фридман О. «Гибридная война» понятий. 2017.
10. Pynnöniemi, Katri. Information-Psychological Warfare in Russian Security Strategy. 2019.
11. Wijermars, Mariëlle. Selling Internet Control: The Framing of the Russian Ban of Messaging App Telegram. Information, Communication & Society, 2022.
12. Russia: Freedom on the Net 2019 Country Report. Freedom House, 2019.
13. Russia’s “Sovereign Internet” Law. Internet Society, 2023.