

RAQAMLI EVOLYUTSIYA VA KIBER-TAHDIDLAR: ZAMONAVIY JAMIYATGA TA'SIRI VA HIMOYA STRATEGIYALARI

Mo'minov Haydar Muhiddinovich

“Realsoft Academy” MChJ direktori, ilmiy rahbar

E-mail: univorarsa@gmail.com

Isomiddinov Jasur Otabek o'g'li

Toshkent Amaliy fanlar Universiteti, Kompyuter injiniringi yo'nalishi

E-mail: isomiddinovjasur23@gmail.com

Alijonov Jasurbek Kamoliddin o'g'li

Toshkent Amaliy fanlar Universiteti, Kompyuter injiniringi yo'nalishi

E-mail: jasurbekaljonov386@gmail.com

ANNOTATSIYA

Ushbu maqolada raqamli evolyutsiya jarayonining jadal rivojlanishi sharoitida kiber-tahdidlarning kuchayishi va ularning zamonaviy jamiyatga ta'siri ilmiy-metodologik jihatdan tahlil qilinadi. Raqamli texnologiyalar, internet infratuzilmasi va sun'iy intellekt asosidagi tizimlarning keng qo'llanilishi natijasida yuzaga kelayotgan xavfsizlik muammolari ko'rib chiqiladi. Maqolada zararli dasturlar, phishing hujumlari, DDoS hujumlari, ransomware va ma'lumotlar o'g'irlanishi kabi asosiy kiber-tahdid turlari tasniflab yoritiladi. Shuningdek, kiberxavfsizlikni ta'minlashning zamonaviy usullari — kuchli autentifikatsiya, shifrlash texnologiyalari, tarmoq monitoringi va foydalanuvchi xabardorligini oshirish — tahlil etiladi. Raqamli evolyutsiya bosqichlari va ularga mos tahdidlar qiyosiy jadval shaklida taqdim etilib, har bir davrdagi xavfsizlik muammolariga kompleks yechimlar tavsiya etiladi. Tadqiqot O'zbekiston raqamli strategiyasi doirasida milliy kiberxavfsizlik tizimini mustahkamlashga doir amaliy tavsiyalarni o'z ichiga oladi.

Kalit so'zlar: raqamli evolyutsiya, kiberxavfsizlik, kiber-tahdidlar, phishing, DDoS, zararli dasturlar, ma'lumotlar himoyasi, shifrlash, autentifikatsiya, kiberjinoyatchilik, raqamli transformatsiya.

ABSTRACT

This paper analyzes the rapid progression of digital evolution and the corresponding intensification of cyber threats in modern society. It examines the security challenges emerging from the widespread adoption of digital technologies, internet infrastructure, and artificial intelligence-based systems. Key cyber threat categories — including malware, phishing, DDoS attacks, ransomware, and data breaches — are systematically classified and discussed. The study further explores modern cybersecurity approaches such as multi-factor authentication, encryption technologies, network monitoring, and user awareness training. A comparative analysis of digital evolution stages and their associated threat landscapes is presented in tabular form, with comprehensive defense recommendations for each period. The research includes practical recommendations for strengthening Uzbekistan's national cybersecurity framework within the scope of its digital development strategy.

Keywords: digital evolution, cybersecurity, cyber threats, phishing, DDoS, malware, data protection, encryption, authentication, cybercrime, digital transformation.

1. KIRISH

XXI asrda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida jamiyatning deyarli barcha sohalarida raqamli transformatsiya jarayoni kuzatilmoqda. Ushbu jarayon ilmiy adabiyotlarda raqamli evolyutsiya tushunchasi bilan izohlanib, inson faoliyati,

iqtisodiyot, davlat boshqaruvi, ta'lim va biznes tizimlarining raqamli muhitga moslashuvi bilan tavsiflanadi. Internet tarmoqlari, bulutli hisoblash, sun'iy intellekt, Big Data va IoT kabi zamonaviy texnologiyalar global rivojlanishning asosiy omillaridan biriga aylangan.

Jahon iqtisodiy forumi va UNESCO hisobotlarida ta'kidlanganidek, raqamli texnologiyalar iqtisodiy samaradorlikni oshirish bilan birga, yangi ijtimoiy va xavfsizlik muammolarini ham yuzaga keltirmoqda (WEF, 2023). Xalqaro telekommunikatsiya ittifoqi (ITU) ma'lumotlariga ko'ra, kiberjinoyatchilik bugungi kunda global iqtisodiyotga yiliga 8 trillion dollardan ortiq zarar yetkazayotgan global tahdidga aylangan. Raqamli infratuzilmaning kengayishi bilan birga zararli dasturlar, phishing, ransomware va DDoS hujumlarining soni yil sayin o'sib bormoqda.

Ushbu maqolaning maqsadi raqamli evolyutsiya jarayonini bosqichma-bosqich tahlil qilish, zamonaviy kiber-tahdidlar turlarini tizimli ravishda tasniflash hamda ulardan himoyalashning kompleks strategiyalarini ko'rib chiqishdan iborat. Maqola O'zbekiston raqamli rivojlanish strategiyasi doirasida milliy kiberxavfsizlik tizimini mustahkamlashga doir amaliy tavsiyalar bilan yakunlanadi.

2. ADABIYOTLAR SHARHI VA NAZARIY ASOS

2.1 Raqamli Evolyutsiya: Tarixiy Nuqtai Nazar

Raqamli evolyutsiya tushunchasi ilmiy adabiyotlarda turlicha talqin etiladi. Westerman va boshqalar (2014) raqamli transformatsiyani tashkilotlar va jamiyatning texnologik imkoniyatlaridan foydalanib asosiy faoliyatni qayta ko'rib chiqishi sifatida belgilaydi. Schwab (2016) to'rtinchi sanoat inqilobi doirasida raqamli, jismoniy va biologik tizimlarning qo'shilishini asosiy xususiyat sifatida ko'rsatadi. O'zbekistonda "Raqamli O'zbekiston — 2030" strategiyasi doirasida axborot-kommunikatsiya texnologiyalarini barcha sohalarga joriy etish ustuvor yo'nalish sifatida belgilangan.

2.2 Kiber-Tahdidlar Landshafti

Kiber-tahdidlar sohasidagi tadqiqotlar shuni ko'rsatadiki, hujumchilar tobora murakkab va avtomatlashtirilgan usullardan foydalanmoqda. Anderson va boshqalar (2019) kiberjinoyatchilik iqtisodiy modeli tadqiqotida fishing va ransomware hujumlarining global moliyaviy zarari yilik hajmini o'rganib, chiqim va foyda nisbatini asosiy omil sifatida ajratib ko'rsatdi. Apruzzese va boshqalar (2022) sun'iy intellektni kiberhujumlarda qo'llash tendensiyalarini tahlil qilib, adversarial ML hujumlarining xavfsizlik tizimlarini aylanib o'tish imkoniyatini ko'rsatdi.

ENISA (2022) tahdidlar landshafti hisobotida ransomware (birinchi o'rinda), ma'lumotlar sizishi, DDoS va supply chain hujumlari eng xavfli tahdidlar ro'yxatida keltirilgan. Verizon (2023) ma'lumotlar buzilishi tadqiqotiga ko'ra, hujumlarning 74% da inson omili — xodimlarning xato harakatlari, ijtimoiy muhandislik yoki credential o'g'irlash — hal qiluvchi rol o'ynagan.

2.3 O'zbekiston Konteksti

Mahalliy adabiyotlar tahlili shuni ko'rsatadiki, O'zbekistonda kiberxavfsizlik sohasidagi ilmiy tadqiqotlar rivojlanish bosqichida. Qosimov (2018), Karimov (2020) va Yo'ldoshev (2021) asarlarida axborot xavfsizligining nazariy asoslari, tarmoq himoyasi va kiberjinoyatchilikka qarshi kurash usullari yoritilgan. G'ulomov va Shermuhamedov (2019) axborot tizimlari va texnologiyalari bo'yicha keng qamrovli qo'llanmani nashr etib, mahalliy ta'lim muassasalarida foydalanilmoqda. Biroq zamonaviy tahdidlar — AI asosidagi hujumlar, supply chain xavfsizligi — mahalliy adabiyotlarda yetarli darajada yoritilmagan.

3. TADQIQOT METODOLOGIYASI

3.1 Tadqiqot Dizayni

Ushbu tadqiqot sifatli keng qamrovli adabiyotlar tahlili va qiyosiy tahlil metodologiyasiga asoslanadi. Tadqiqot ikki qatlamdan iborat: (1) raqamli evolyutsiya bosqichlari va ularga mos tahdidlar landshaftini tarixiy-qiyosiy tahlil qilish; (2) zamonaviy kiber-tahdidlar va himoya mexanizmlarini tizimli tasniflash va baholash.

3.2 Ma'lumotlar Manbalari

Tadqiqotda quyidagi manba toifalari qo'llanildi:

Xalqaro ilmiy ma'lumotlar bazalari: IEEE Xplore, ACM Digital Library, Scopus, Google Scholar — 2019–2024 yillar orasidagi peer-reviewed maqolalar.

Xalqaro tashkilot hisobotlari: ITU, ENISA, WEF, Verizon DBIR, IBM Security.

Milliy manbalar: O'zbekiston Respublikasi qonunchiligi, "Raqamli O'zbekiston" strategiyasi, mahalliy ilmiy nashrlar.

Texnik standartlar: NIST Cybersecurity Framework, ISO/IEC 27001, OWASP Top 10.

3.3 Axloqiy Mulohazalar

Tadqiqot jarayonida shaxsiy ma'lumotlar yoki maxfiy tijorat ma'lumotlaridan foydalanilmagan. Barcha ko'rsatkichlar ochiq nashr etilgan manbalardan olingan. Tadqiqot akademik halollik tamoyillariga muvofiq olib borilgan va barcha manbalar to'g'ri iqtibos qilingan.

4. NATIJALAR VA MUHOKAMA

4.1 Raqamli Evolyutsiya Bosqichlari va Tahdidlar

Raqamli evolyutsiya to'rt asosiy bosqichda ko'rib chiqilishi mumkin bo'lib, har bir bosqichga xos texnologiyalar va ularga mos kiber-tahdidlar quyidagi jadvalda keltirilgan:

Jadval 1. Raqamli Evolyutsiya Bosqichlari va Kiber-Tahdidlar Dinamikasi

Davr	Bosqich	Texnologiyalar	Asosiy tahdidlar
1960–1980	Kompyuterlash	Hisoblash texnikasi joriy etish	Cheklangan tarmoq hujumlari
1980–2000	Internetlashtirish	Global tarmoqlar, e-tijorat	Viruslar, worms, spam
2000–2015	Raqamli xizmatlar	Bulut, mobil, ijtimoiy tarmoq	Phishing, DDoS, APT
2015–hozir	Raqamli transformatsiya	AI, IoT, Big Data, 5G	Ransomware, deepfake, AI hujumlar

Jadvaldan ko'rinib turibdiki, raqamli evolyutsiya qanchalik chuqurlashsa, kiber-tahdidlar shunchalik murakkablashmoqda. AI texnologiyalarining joriy etilishi bilan tahdidlar yangi bosqichga — avtonom, moslashuvchan va keng ko'lamli hujumlarga — o'tmoqda.

4.2 Zamonaviy Kiber-Tahdidlar Tasnifi

Quyidagi jadvalda zamonaviy kiber-tahdidlarning asosiy turlari, mexanizmlari, oqibatlari va himoya usullari tizimli ravishda taqdim etiladi:

Jadval 2. Zamonaviy Kiber-Tahdidlar: Tasnif va Himoya Usullari

Tahdid turi	Mexanizm	Oqibati	Himoya
Zararli dasturlar	Virus, troyan, qurt, spyware	Tizimni buzish, ma'lumot o'g'irlash	Antivirus, sandbox
Phishing	Soxta email, veb-sayt	Parol, karta ma'lumotlari	MFA, xodim treningi
DDoS hujumi	Botnet, amplifikatsiya	Xizmatni to'xtatish	CDN, trafikni filtrlash
Ransomware	Shifrlash + tovlamachilik	Moliyaviy zarar, ma'lumot yo'qotish	Zaxira, Zero Trust
Ma'lumot sizishi	SQL injection, insayder	Maxfiylik buzilishi	DLP, kirish nazorati
APT	Uzoq muddatli josuslik	Davlat/korporativ ma'lumot	SIEM, anomaliya tahlili

Ransomware hujumlari ayniqsa katta zarar yetkazmoqda. IBM (2023) ma'lumotlariga ko'ra, o'rtacha ma'lumotlar buzilishi xarajati 4.45 million dollarga yetib, so'nggi 3 yilda 15% ga oshgan. Phishing esa hujumlarning 36% dan ortig'ining kirish nuqtasi bo'lib, inson omiliga tayanishi uni texnik himoya choralaridan alohida turuvchi tahdidga aylantiradi.

4.3 Raqamli Evolyutsiyaning Jamiyatga Ta'siri

Raqamli evolyutsiya ijobiy tomonlari bilan birga bir qator jiddiy muammolarni ham keltirib chiqarmoqda. Ma'lumotlar maxfiyligi masalasi GDPR kabi qonunchilik hujjatlarining qabul qilinishiga sabab bo'ldi. O'zbekistonda "Shaxsiy ma'lumotlar to'g'risida" Qonun (2019) va "Axborot xavfsizligi to'g'risida" Qonun (2022) bu yo'nalishdagi asosiy me'yoriy hujjatlar hisoblanadi.

Sun'iy intellekt texnologiyalarining rivojlanishi kiberhujumlarning yanada murakkab shakllarini — deepfake asosidagi fishing, avtomatlashtirilgan zaifliklarni aniqlash, polimorf zararli dasturlar — yuzaga keltirmoqda. IoT qurilmalarining keng tarqalishi hujum yuzasini keskin kengaytirib, an'anaviy perimetr himoyasini samarasiz qilmoqda. Bulut infratuzilmasiga o'tish esa umumiy javobgarlik modelini tushunmaslik natijasida yuzaga keladigan noto'g'ri konfiguratsiya xatolarini asosiy zaiflikka aylantirdi.

4.4 Kiberxavfsizlikni Ta'minlash Strategiyalari

Zamonaviy kiberxavfsizlik ko'p qatlamli (defense-in-depth) yondashuvga asoslanishi zarur. Asosiy strategik elementlar quyidagilardan iborat:

Ko'p faktorli autentifikatsiya (MFA): parollarga asoslangan himoyani kuchaytirib, hisob o'g'irlanishini 99.9% gacha kamaytiradi (Microsoft, 2023).

Shifrlash: saqlangan va uzatilayotgan ma'lumotlar uchun AES-256 va TLS 1.3 standartlari qo'llanilishi zarur.

Zero Trust arxitekturasini: "hech kimga ishonma, hammasini tekshir" tamoyili asosida tarmoq ichidagi lateral harakatni cheklash.

Xavfsizlik devori va IDS/IPS: tarmoqqa kirish-chiqishni nazorat qilish va anomaliyalarni real vaqtda aniqlash.

Muntazam yangilanishlar va patch menejmenti: ma'lum zaifliklarning 60% i mavjud patchlarni o'rnatish orqali bartaraf etilishi mumkin (CISA, 2022).

Xodimlar treningi: ijtimoiy muhandislik hujumlariga qarshi eng samarali vosita — xodimlarning xabardorligi va tayyorgarligi.

Hodisalarga javob berish rejasi (Incident Response Plan): hujum sodir bo'lganda tizimli va tezkor munosabatni ta'minlash.

5. TADQIQOT CHEKLOVLARI

Ushbu tadqiqotning bir necha muhim cheklovlari mavjud. Birinchidan, maqola asosan nashr etilgan adabiyotlar va ochiq hisobotlarga tayanib, amaliy sinov yoki so'rovnoma o'tkazmagan. Bu esa empirik ma'lumotlar bilan nazariy tahlilni to'ldirish zarurligini ko'rsatadi. Ikkinchidan, kiberxavfsizlik sohasi juda tez o'zgaruvchan bo'lib, maqolada keltirilgan ba'zi ko'rsatkichlar tez o'zgarishi mumkin — shu sababli doimiy monitoring va yangilanib boruvchi adabiyotlar tahlili zarur.

Uchinchidan, O'zbekiston bo'yicha maxsus empirik ma'lumotlar — kiberhujumlar soni, moliyaviy zararlar, sektoral taqsimot — hali cheklangan darajada ochiq manbalarda mavjud. To'rtinchidan, industrial boshqaruv tizimlari (ICS/SCADA), tibbiyot tizimchilari va moliya sektori kabi maxsus tarmoqlar ushbu maqolada chuqur ko'rib chiqilmagan. Kelajakdagi tadqiqotlar ushbu bo'shliqlarni to'ldirish uchun O'zbekistondagi tashkilotlar bilan hamkorlikda amaliy tadqiqotlar o'tkazishi tavsiya etiladi.

6. XULOSA VA TAKLIFLAR

Raqamli evolyutsiya zamonaviy jamiyat taraqqiyotining ajralmas qismi bo'lib, iqtisodiyot, ta'lim, sog'liqni saqlash va davlat boshqaruvida beqiyos imkoniyatlar yaratmoqda. Biroq ushbu jarayon bilan parallel ravishda kiber-tahdidlarning soni, murakkabligi va moliyaviy zarari ham tez sur'atlarda ortib bormoqda. Ushbu tadqiqot uchta asosiy xulosani tasdiqladi:

Raqamli evolyutsiya har bir yangi bosqichda yangi tahdidlar sinfi bilan birga keladi — kompyuterlashtirish viruslarni, internetlashtirish fishingni, AI esa avtonom va adaptiv hujumlarni keltirib chiqardi.

Inson omili — xodimlarning xato harakatlari va ijtimoiy muhandislikka moyilligi — hujumlarning 74% da muhim rol o'ynamoqda va texnik himoya choralarini yetarli emasligi isbotlangan.

Kompleks, ko'p qatlamli kiberxavfsizlik strategiyasi — Zero Trust, MFA, shifrlash, xodimlar treningi va hodisalarga javob berish rejasini o'z ichiga olgan — eng samarali himoya yondashuvi hisoblanadi.

Amaliy tavsiyalar sifatida quyidagilar taklif etiladi:

O'zbekiston tashkilotlari uchun milliy kiberxavfsizlik etukligi modeli (CMM) ishlab chiqish va joriy etish.

Davlat va xususiy sektor o'rtasida kiber-tahdidlar bo'yicha axborot almashish platformasini yaratish.

Oliy ta'lim muassasalarida kiberxavfsizlik fanini majburiy kurs sifatida joriy etish va amaliy laboratoriyalar tashkil etish.

CERT (Computer Emergency Response Team) tarmog'ini kengaytirish va sohaviy CERT markazlarini barpo etish.

Post-kvant kriptografiyasiga o'tish rejasini hozirdan tuzib, milliy infratuzilmani tayyorlashni boshlash.

7. ADABIYOTLAR RO'YXATI (APA 7 FORMATI)

- [1] Anderson, R., Barton, C., Böhme, R., Clayton, R., Ganan, C., Grasso, T., ... & Vasek, M. (2019). Measuring the changing cost of cybercrime. The 18th Workshop on the Economics of Information Security (WEIS 2019).
- [2] Apruzzese, G., Colajanni, M., Ferretti, L., & Marchetti, M. (2022). Revisiting the limitations of deep learning for intrusion detection and the potential of adversarial machine learning. Proceedings of the 2022 International Conference on Information and Communications Security, 41–57. https://doi.org/10.1007/978-3-031-15777-6_3
- [3] CISA. (2022). Known exploited vulnerabilities catalog. Cybersecurity and Infrastructure Security Agency. <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- [4] European Union Agency for Cybersecurity (ENISA). (2022). ENISA threat landscape 2022. <https://doi.org/10.2824/764318>
- [5] G'ulomov, S. S., & Shermuhamedov, A. T. (2019). Axborot tizimlari va texnologiyalari. Iqtisod-Moliya.
- [6] IBM Security. (2023). Cost of a data breach report 2023. IBM Corporation. <https://www.ibm.com/reports/data-breach>
- [7] International Telecommunication Union (ITU). (2022). Global cybersecurity index 2020. ITU Publications. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>
- [8] Karimov, A. A. (2020). Kiberxavfsizlik va axborot himoyasi. Fan va texnologiya.
- [9] Microsoft. (2023). Digital defense report 2023. Microsoft Corporation. <https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023>
- [10] O'zbekiston Respublikasi. (2020). Axborot xavfsizligi to'g'risida qonun. O'zbekiston Respublikasi Qonun hujjatlari ma'lumotlari milliy bazasi. <https://lex.uz>
- [11] O'zbekiston Respublikasi Prezidenti Farmoni. (2020). "Raqamli O'zbekiston — 2030" strategiyasini tasdiqlash to'g'risida. <https://lex.uz>
- [12] Qosimov, S. S. (2018). Axborot xavfsizligi asoslari. Aloqachi.
- [13] Schwab, K. (2016). The fourth industrial revolution. World Economic Forum.
- [14] Verizon. (2023). 2023 data breach investigations report. Verizon Business. <https://www.verizon.com/business/resources/reports/dbir/>
- [15] Westerman, G., Bonnet, D., & McAfee, A. (2014). Leading digital: Turning technology into business transformation. Harvard Business Review Press.
- [16] World Economic Forum (WEF). (2023). Global cybersecurity outlook 2023. <https://www.weforum.org/reports/global-cybersecurity-outlook-2023/>
- [17] Xolmatov, N. N. (2020). Kiberjinoyatchilik va unga qarshi kurashish usullari. Yuridik adabiyotlar nashriyoti.
- [18] Yo'ldoshev, M. M. (2021). Kompyuter tarmoqlari va axborot xavfsizligi. O'zbekiston.