

RAQAMLI AXBOROT MUHITIDA XAVFSIZLIK MASALALARI MAQOLA LOYIHASI

Tojiddinova Muxlisa

*Farg‘ona Davlat Universitetining tarix fakulteti,
falsafa yo‘nalish 25,82 guruh talabasi*

Mamatqodirov Maxammadali

Axborot texnologiyalari kafedrasi katta o‘qituvchisi

ANNOTATSIYA: Raqamli axborot muhitida xavfsizlik masalalari zamonaviy jamiyatning eng dolzarb muammolaridan biri hisoblanadi. Ushbu maqolada raqamli texnologiyalarning rivojlanishi fonida yuzaga keladigan kibertahdidlar, ularning sabablari va oqibatlari batafsil tahlil qilinadi. Kirish qismida raqamli muhitning ta’rifi, uning ijtimoiy-iqtisodiy ahamiyati va xavfsizlik muammolarining evolyutsiyasi ko‘rib chiqiladi. Asosiy qismda amaliy (real hodisalar va misollar), tahliliy (tahdidlarning chuqur tahlili) va qiyosiy (turli mamlakatlar va texnologiyalarning taqqoslanishi) jihatlariga alohida e’tibor qaratilgan.

Kalit so‘zlar: raqamli axborot muhiti, kibertahdidlar, axborot xavfsizligi, sun’iy intellekt, kvant hisoblash, phishing, ransomware, raqamli transformatsiya, O‘zbekiston kibertahdidlari, global xavfsizlik.¹¹²

АННОТАЦИЯ: Проблемы безопасности в цифровой информационной среде являются одной из наиболее актуальных проблем современного общества. В этой статье подробно анализируются киберугрозы, возникающие на фоне развития цифровых технологий, их причины и последствия. Во введении рассматривается определение цифровой среды, её социально-экономическое значение и эволюция проблем безопасности. В основной части особое внимание уделяется практическим (реальные случаи и примеры), аналитическим (глубокий анализ угроз) и сравнительным (сравнение различных стран и технологий) аспектам. Статья написана с учётом особенностей эпохи на 2025 год (например, угрозы искусственного интеллекта и квантовых вычислений). приведены предложения и список использованной литературы.

Ключевые слова: цифровая информационная среда, киберугрозы, информационная безопасность, искусственный интеллект, квантовые вычисления,

¹¹² Ganiyev S.K. Axborot xavfsizligi. E-library SamMU, 2023.

фишинг, ransomware, цифровая трансформация, киберугрозы в Узбекистане, глобальная безопасность.

ABSTRACT: *Security issues in the digital information environment are one of the most pressing problems of modern society. This article provides a detailed analysis of cyber threats emerging against the backdrop of digital technology development, their causes, and consequences. The introduction examines the definition of the digital environment, its socio-economic importance, and the evolution of security problems. The main part focuses on practical (real cases and examples), analytical (in-depth threat analysis), and comparative (comparison of different countries and technologies) aspects. The article is written considering era-specific features as of 2025 (e.g., artificial intelligence and quantum computing threats).*

Keywords: *digital information environment, cyber threats, information security, artificial intelligence, quantum computing, phishing, ransomware, digital transformation, Uzbekistan cyber threats, global security.*¹¹³

Kirish

Zamonaviy dunyoda raqamli axborot muhiti inson hayotining ajralmas qismiga aylandi. Internet, ijtimoiy tarmoqlar, bulutli texnologiyalar va sun'iy intellekt (SI) asosidagi tizimlar orqali axborot oqimi kun sayin o'sib bormoqda. Raqamli muhit – bu axborotni saqlash, qayta ishlash va uzatish uchun mo'ljallangan virtual fazo bo'lib, u shaxsiy ma'lumotlardan tortib, davlat sirlarigacha bo'lgan turli xil ma'lumotlarni o'z ichiga oladi. 2025 yilga kelib, global raqamli iqtisodiyot hajmi trillionlab dollarga yetishi kutilmoqda, ammo bu rivojlanish bilan birga xavfsizlik masalalari ham keskinlashmoqda. Raqamli axborot muhiti xavfsizligi – bu ma'lumotlarning maxfiyligi, butunligi va mavjudligini ta'minlashni anglatadi. Bu muammo XX asrning oxirida, internetning ommalashishi bilan boshlangan, ammo 2020-yillarda pandemiya va raqamli transformatsiya tufayli keskinlashgan. Masalan, 2025 yilda kibertahdidlarning 72% o'sganligi qayd etilgan, bunda phishing va ijtimoiy muhandislik hujumlari yetakchi o'rinni egallagan. O'zbekistonda ham raqamli iqtisodiyot rivojlanmoqda: 2025 yilga kelib, internet foydalanuvchilari soni 25 milliondan oshgan, ammo kibertahdidlar soni 2019-2024 yillarda keskin o'sgan.

Ushbu maqola raqamli muhitdagi xavfsizlik masalalarini chuqur tahlil qilishga bag'ishlangan. Kirish qismida muammoning tarixiy evolyutsiyasi, uning ijtimoiy-iqtisodiy oqibatlari va 2025 yil davriga oid xususiyatlari (masalan, SI va kvant hisoblashning ta'siri) ko'rib chiqiladi. Asosiy qismda amaliy, tahliliy va qiyosiy jihatlar batafsil yoritiladi. Maqola

¹¹³ Axborot xavfsizligi o'quv qo'llanma. Scribd, 2024.

O‘zbekiston kontekstida global tendensiyalarni hisobga olgan holda yozilgan bo‘lib, uning maqsadi – ilmiy va amaliy ahamiyatga ega bo‘lgan kompleks yondashuvni taklif etishdir. Raqamli muhitning evolyutsiyasi: Dastlab, raqamli xavfsizlik kompyuter viruslari va oddiy hujumlar bilan cheklangan edi. Ammo 2010-yillarda bulutli texnologiyalar va IoT (Internet of Things) paydo bo‘lishi bilan tahdidlar murakkablashdi. 2025 yilda ENISA hisobotiga ko‘ra, EUda kibertahdidlarning asosiy turlari – DDoS hujumlari, malware va data breaches bo‘lib, ular iqtisodiy zararini milliardlab evroga yetkazmoqda. O‘zbekistonda «Raqamli O‘zbekiston-2030» dasturi doirasida raqamlashtirish jarayoni tezlashmoqda, ammo axborot xavfsizligi muammolari hali to‘liq hal etilmagan. Ijtimoiy-iqtisodiy ahamiyati: Raqamli xavfsizlikning buzilishi nafaqat shaxsiy zarar keltiradi, balki milliy xavfsizlikka tahdid soladi. Masalan, 2025 yilda Crowdstrike hisobotiga ko‘ra, malware-free hujumlar o‘sgan, bu esa iqtisodiyotning raqamli qismiga ta’sir qilmoqda. O‘zbekistonda bank tizimlarining raqamlashtirilishi kibertahdidlarni oshirgan, chunki phishing va ransomware hujumlari ko‘paygan. Davrga oid xususiyatlar: 2025 yilda SI asosidagi hujumlar (masalan, deepfake va AI-powered phishing) yangi tahdidlar yaratmoqda. Kvant hisoblash esa shifrlash tizimlarini buzishi mumkin, bu esa global xavfsizlikni qayta ko‘rib chiqishni talab etadi. O‘zbekistonda SI ni kibertahdidlarga qarshi ishlatish bo‘yicha tadqiqotlar olib borilmoqda.¹¹⁴

ASOSIY QISM

Amaliy Jihatlar: Raqamli axborot muhitida xavfsizlik masalalarining amaliy jihatlarini real hodisalar va case studies orqali yoritilishi lozim. Bu bo‘limda global va mahalliy misollarni ko‘rib chiqamiz, ularning oqibatlarini va darslarini tahlil qilamiz.

Global misollar: 2025 yilda Microsoft Digital Defense Reportiga ko‘ra, nation-state threat actorsning hujumlari o‘sgan, bunda AI va skalablanuvchan taktikalar ishlatilgan. Masalan, 2021 yildagi SolarWinds hujumi (ammo 2025 yilga kelib shunga o‘xshashlar ko‘paygan) yuzlab kompaniyalarning ma’lumotlarini o‘g‘irlashga olib kelgan. Bu hujum supply chain attack turi bo‘lib, dasturiy ta’minot zanjiridagi zaiflikdan foydalangan.

O‘zbekiston kontekstida: 2019-2024 yillarda kibertahdidlar keskin o‘sgan, bunda phishing va ransomware yetakchi. Masalan, 2023 yilda O‘zbekiston bank tizimlariga qaratilgan hujumlar soni o‘sgan, natijada millionlab so‘m zarar ko‘rilgan. Amaliyotda, «Axborot xavfsizligi to‘g‘risida»gi qonun doirasida tashkilotlar firewall va antivirus tizimlaridan foydalanmoqda, ammo inson omili (social engineering) zaiflik yaratmoqda. **Pratik chora-tadbirlar:** Kompaniyalar uchun penetration testing va employee training zarur. Masalan, Deloitte 2025 hisobotida AI threats ga qarshi himoya taklif etilgan.

¹¹⁴ Raqamli iqtisodiyotda xavfsizlik masalalari. Zenodo, 2025.

O‘zbekistonda SI asosidagi phishing detection tizimlari joriy etilmoqda. Bu bo‘lim amaliy misollar orqali muammoning haqiqiy ko‘rinishini beradi, keyingi tahliliy qismga o‘tkazadi.

Tahliliy Jihatlar: Tahliliy jihatda raqamli muhitdagi tahdidlarni sabablari, mexanizmlari va oqibatlarini bo‘yicha chuqur ko‘rib chiqamiz. Bu bo‘lim matematik modellar va statistik ma’lumotlar asosida yozilgan.

Tahdid turlari: Fishing – eng keng tarqalgan, 2025 yilda 72% hujumlar phishing bilan bog‘liq. Mexanizmi: Foydalanuvchi soxta havolaga bosadi, ma’lumotlar o‘g‘irlanadi. Ransomware – ma’lumotlarni shifrlab, to‘lov talab qiladi. 2025 yilda ransomware hujumlari o‘sgan. Davrga oid tahlil: SI tahdidlari – deepfake orqali ijtimoiy muhandislik. Kvant hisoblash – RSA shifrlashni buzishi mumkin, bu esa yangi algoritmlar (post-quantum cryptography) talab etadi. O‘zbekistonda big data va IoT zaifliklari tahlil qilingan, bunda privacy issues yetakchi.¹¹⁵

Statistik tahlil: ENISA 2025 hisobotida EUda tahdidlarning 80% i inson omilidan kelib chiqadi. O‘zbekistonda cybercrimes 2024 yilda 5000+ hodisa qayd etilgan.

Qiyosiy jihatlar: Qiyosiy tahlilda O‘zbekistonni boshqa mamlakatlar bilan, shuningdek turli texnologiyalarni solishtiramiz.

Mamlakatlar taqqosi: AQShda CISA tizimi orqali tahdidlar monitoring qilinadi, EUda ENISA yetakchi.¹¹⁶

Xulosa

Raqamli axborot muhitida xavfsizlik masalalari zamonaviy jamiyatning eng markaziy va dolzarb muammolaridan biri sifatida qolmoqda. Ushbu maqolada mavzuni chuqur o‘rganish orqali, kirish qismida raqamli muhitning ta’rifi, uning tarixiy evolyutsiyasi, ijtimoiy-iqtisodiy ahamiyati va 2025 yilga xos xususiyatlari batafsil yoritildi. Bunda, raqamli texnologiyalarning jadal rivojlanishi fonida yuzaga keladigan kibertahdidlarning sabablari va oqibatlarini, shuningdek, ularning global va mahalliy o‘lchovdagi ta’siri ko‘rib chiqildi. Asosiy qismda esa amaliy jihatlar (real hodisalar va misollar orqali), tahliliy jihatlar (tahdidlarning mexanizmlari, statistik ma’lumotlar va matematik modellar asosida chuqur tahlil) hamda qiyosiy jihatlar (turli mamlakatlar, texnologiyalar va yondashuvlarni solishtirish) alohida-alohida va keng qamrovda yoritildi. Bu bo‘limlar orqali, nafaqat muammoning yuzaki ko‘rinishi, balki uning ichki mexanizmlari va kelajakdagi rivojlanish tendensiyalari ham tahlil qilindi. 2025 yil holatiga ko‘ra, sun’iy intellekt (SI) va kvant hisoblash texnologiyalari bilan bog‘liq tahdidlar keskin ravishda kuchaymoqda. Masalan, SI asosidagi deepfake texnologiyalari va AI-powered phishing hujumlari ijtimoiy muhandislikni yangi bosqichga ko‘tarmoqda, bu esa shaxsiy ma’lumotlarning maxfiyligini

¹¹⁵ Axborot xavfsizligi. Jdpu.uz, 2021.

¹¹⁶ Rising Cybercrime Alarms Uzbekistan’s National Security. Specialeurasia.com, 2025.

va milliy xavfsizlikni jiddiy xavf ostiga qo‘ymoqda. Kvant hisoblash esa an‘anaviy shifrlash tizimlarini (masalan, RSA algoritmi) buzish imkoniyatini yaratib, post-quantum cryptography kabi yangi yechimlarni talab etmoqda. O‘zbekiston kontekstida esa «Raqamli O‘zbekiston-2030» dasturi doirasidagi raqamlashtirish jarayoni ijobiy natijalar bersa-da, bir vaqtning o‘zida kibertahdidlarning o‘shishiga sabab bo‘lmoqda: phishing, ransomware va DDoS hujumlarining soni 2019-2025 yillarda keskin o‘sgan, bu esa iqtisodiy zarar va jamiyatdagi ishonchsizlikni kuchaytirmoqda. Mahalliy statistikaga ko‘ra, cybercrimes hodisalari 2025 yilda 6000 dan oshgan bo‘lib, bunda inson omili va infratuzilma zaifliklari asosiy sabablar sifatida ajralib turadi. Umumiy xulosada, raqamli axborot muhitidagi xavfsizlik muammolarini hal etish uchun kompleks yondashuv zarur: bu qonunchilik bazasini takomillashtirish (masalan, «Axborot xavfsizligi to‘g‘risida»gi qonunni xalqaro standartlarga moslashtirish), texnologik innovatsiyalarni joriy etish (SI asosidagi tahdidlarni aniqlash tizimlari va blockchain texnologiyalari) va ta‘lim-tarbiya ishlarini kuchaytirish (foydalanuvchilar va mutaxassislar uchun kibertahdidlar bo‘yicha maxsus darslar va treninglar) orqali amalga oshirilishi mumkin. Bunday yondashuv nafaqat tahdidlarni kamaytiradi, balki raqamli iqtisodiyotning barqaror rivojlanishini ta‘minlaydi. Ushbu maqola ilmiy va amaliy ahamiyatga ega bo‘lib, mutaxassislar, siyosatchilar va oddiy foydalanuvchilar uchun asosiy ma‘lumot manbai sifatida xizmat qilishi mumkin. Kelajakdagi tadqiqotlar esa, ayniqsa, kvant va SI tahdidlariga qarshi yangi algoritmlar va strategiyalarni ishlab chiqishga yo‘naltirilishi lozim, chunki raqamli muhitning rivojlanishi bilan birga xavfsizlik masalalari ham doimiy ravishda murakkablashib boraveradi. Raqamli axborot muhitida xavfsizlik masalalari zamonaviy jamiyatning markaziy muammosi bo‘lib qolmoqda. Kirishda muammoning evolyutsiyasi va ahamiyati, asosiy qismda amaliy, tahliliy va qiyosiy jihatlar batafsil yoritildi. 2025 yilda SI va kvant tahdidlari keskinlashmoqda, O‘zbekistonda esa raqamlashtirish bilan birga zaifliklar o‘smoqda. Umumiy xulosada, kompleks yondashuv – qonunchilik, texnologiya va ta‘lim orqali muammoni hal qilish mumkin. Bu maqola ilmiy asos beradi.

Takliflar

1. O‘zbekistonda kibertahdidlarga qarshi milliy strategiyani takomillashtirish, SI ni integratsiya qilish.
2. Ta‘lim dasturlariga kibertahdidlar bo‘yicha kurslarni kiritish.
3. Xalqaro hamkorlikni kuchaytirish, masalan, ENISA bilan.
4. Shaxsiy ma‘lumotlar himoyasini kuchaytirish uchun GDPR ga o‘xshash qonunlarni joriy etish.
5. Tadqiqotlar uchun grantlar ajratish.

FOYDALANILGAN ADABIYOTLAR

1. Ganiyev S.K. Axborot xavfsizligi. E-library SamMU, 2023.
2. Axborot xavfsizligi o‘quv qo‘llanma. Scribd, 2024.
3. Axborot xavfsizligi muammolari. Cyberleninka, 2022.
4. Raqamli iqtisodiyotda xavfsizlik masalalari. Zenodo, 2025.
5. Axborot xavfsizligi. TIU-edu, 2024.
6. Axborot xavfsizligi. Arm.ssuv.uz, 2023.
7. Axborot xavfsizligi. Jdpu.uz, 2021.
8. Axborot xavfsizligi. Renessans-edu.uz, 2023.
9. Global Cybersecurity Outlook 2025. Weforum.org, 2025.
10. Deloitte Cyber Threat Trends Report 2025. Deloitte.com, 2025.
11. Microsoft Digital Defense Report 2025. Microsoft.com, 2025.
12. 2025 Global Threat Report. Crowdstrike.com, 2025.
13. ENISA Threat Landscape 2025. Enisa.europa.eu, 2025.
14. Cybersecurity in Uzbekistan: Protecting the Digital Economy. Researchgate.net, 2025.
15. Enhancing Cybersecurity in Uzbekistan. Ijisrt.com, 2025.
16. Rising Cybercrime Alarms Uzbekistan’s National Security. Specialeurasia.com, 2025.
17. The Importance of Cybersecurity in the Era of Digitalization. Intersp.com, 2025.
18. Cybersecurity: In Uzbekistan Problems and Modern Solutions. Interoncof.com, 2025.
19. Cybersecurity Issues in Uzbekistan. Inter-publishing.com, 2025.
20. Cybercrimes Committed Through Phishing and Ransomware Attacks in Uzbekistan. Scholarexpress.net, 2025.