ACUMEN: INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH
ISSN: 3060-4745 IF(Impact Factor)10.71 / 2025 Volume 2, Issue 11

KIBEROLAM: MILLIY XAVFSIZLIKNING YANGI FRONTI

Dexqonboyev Burxoniddin Maxmudjonovich

Milliy universitet axborot xavsizligi yonalishi 2 kurs talabasi

dburxoniddin1@gmail.com

+998940950006

Annotatsiya; Ushbu maqolada zamonaviy kiberxavfsizlik tahdidlari va ularning milliy xavfsizlik tizimiga ta’siri chuqur tahlil qilinadi. Asarda APT (Advanced Persistent Threat) guruhlarining faoliyati, F-35 texnologik o‘g‘irligi misolida kiberurushlarning global oqibatlari, hamda O‘zbekiston Respublikasida kiberxavfsizlik sohasida amalga oshirilayotgan islohotlar ilmiy asosda yoritilgan. Muallif tomonidan taklif etilgan “Milliy Kiberbarqarorlik va Raqamli Suverenitet Modeli (MKRM)” texnologik, iqtisodiy va ijtimoiy omillarni uyg‘unlashtirgan holda milliy kiberxavfsizlik tizimini mustahkamlashga qaratilgan. Model Yagona Kiber Monitoring Markazi, Banklararo Kiber Konsorsium va CyberSafe Schools kabi tashabbuslar orqali davlat, biznes va fuqarolar darajasida barqaror raqamli muhit yaratishni nazarda tutadi. Tadqiqotda aralash metodologik yondashuv, qiyosiy tahlil, SWOT va xavf tahlili usullaridan foydalanilgan bo‘lib, natijalar O‘zbekistonning kiberxavfsizlik bo‘yicha xalqaro reytinglardagi o‘rnini mustahkamlashga xizmat qiladi.

Kalit so‘zlar: kiberxavfsizlik, milliy xavfsizlik, kiberurushlar, APT guruhlari, F-35, raqamli suverenitet, kiberjinoyatlar, raqamli iqtisodiyot, Zero Trust, O‘zbekiston, Milliy Kiberbarqarorlik modeli, UZSOC, raqamli transformatsiya, kiberbarqarorlik, kiberhujumlar.

Abstract: This article provides an in-depth analysis of modern cybersecurity threats and their impact on the national security system. The study examines the activities of APT (Advanced Persistent Threat) groups, the global consequences of cyber warfare illustrated by the F-35 technology theft, and the cybersecurity reforms currently being implemented in the Republic of Uzbekistan. The author proposes the "National Cyber Resilience and Digital Sovereignty Model (NCRDSM)," which integrates technological, economic, and social factors to strengthen the national cybersecurity system. The model aims to create a stable digital environment at the state, business,

and citizen levels through initiatives such as the Unified Cyber Monitoring Center, Interbank Cyber Consortium, and CyberSafe Schools. The study employs a mixed methodological approach, comparative analysis, SWOT, and risk assessment methods, with results aimed at enhancing Uzbekistan's position in international cybersecurity rankings.

Keywords: cybersecurity, national security, cyber warfare, APT groups, F-35, digital sovereignty, cybercrime, digital economy, Zero Trust, Uzbekistan, National Cyber Resilience Model, UZSOC, digital transformation, cyber resilience, cyberattacks.

Аннотация: В данной статье проводится глубокий анализ современных угроз кибербезопасности и их влияния на систему национальной безопасности. Рассматриваются деятельность групп APT (Advanced Persistent Threat), глобальные последствия кибервойн на примере кражи технологий F-35, а также реформы в области кибербезопасности, проводимые в Республике Узбекистан. Автор предлагает «Модель национальной киберустойчивости и цифрового суверенитета (МКРУЦС)», которая объединяет технологические, экономические и социальные факторы для укрепления национальной системы кибербезопасности. Модель предполагает создание стабильной цифровой среды на уровне государства, бизнеса и граждан через такие инициативы, как Единый центр кибермониторинга, Межбанковский киберконсорциум и CyberSafe Schools. В исследовании используется смешанный методологический подход, сравнительный анализ, SWOT-анализ и методы оценки рисков, результаты направлены на укрепление позиции Узбекистана в международных рейтингах кибербезопасности.

Ключевые слова: кибербезопасность, национальная безопасность, кибервойны, группы APT, F-35, цифровой суверенитет, киберпреступность, цифровая экономика, Zero Trust, Узбекистан, Модель национальной киберустойчивости, UZSOC, цифровая трансформация, киберустойчивость, кибератаки.

Metodologiya

Ushbu "Kiberolam: Milliy Xavfsizlikning Yangi Fronti" mavzusidagi tadqiqot, zamonaviy kibertahdidlarning murakkab tabiatini har tomonlama o‘rganish va O‘zbekiston Respublikasi sharoitiga mos "Milliy Kiberbarqarorlik va Raqamli Suverenitet Modeli"ni ishlab chiqish maqsadida tuzilgan qat’iy metodologik asosga ega. Tadqiqotning ilmiy yondashuvi quyidagi tarkibiy qismlardan iborat;

1. Tadqiqot Dizayni va Umumiy Yondashuv; Tadqiqot aralash-uslub (mixed-methods) paradigmasi asosida amalga oshirildi, bu esa sifatli va miqdoriy tahlil usullarini integratsiya qilish imkonini berdi. Sifatli komponent kiberxavfsizlik sohasidagi global tendensiyalar, APT (Advanced Persistent Threat) guruhlarining operatsion taktikalari, O‘zbekistonda olib borilayotgan qonuniy islohotlar va institutsional tashkiliy mexanizmlarni chuqur tahlil qilishga qaratildi. Miqdoriy komponent esa kiberhujumlar dinamikasi, iqtisodiy zarar ko‘rsatkichlari, xalqaro reytinglar va statistik ma’lumotlar asosida o‘lchovli baholashni o‘z ichiga oldi.

2. Ma’lumotlar Bazasini Shakllantirish va Manbalar Tahlili; Tadqiqotning empirik asosini shakllantirish uchun keng qamrovli ikkilamchi ma’lumotlar manbalari tahlil qilindi. Xalqaro tashkilotlar (ITU, WIPO, GAO, NATO) monitoring hisobotlari, O‘zbekiston Respublikasining "Kiberxavfsizlik to‘g‘risida"gi Qonuni va boshqa normativ-huquqiy hujjatlar, ixtisoslashtirilgan xavfsizlik agentliklarining (Mandiant, CISA) texnik hisobotlari, akademik tadqiqotlar va iqtisodiy tahilllar tanqidiy nuqtai nazardan o‘rganildi. Qiyosiy tahlil metodi orqali AQSh, Rossiya, Xitoy, Ukraina kabi davlatlarning kiberxavfsizlikdagi strategiyalari va tajribalari O‘zbekiston kontekstida solishtirildi.

3. Tadqiqot jarayonida quyidagi tahlil usullari qo‘llanildi: Xavf-tahlil (Risk Assessment) - O‘zbekiston kibermakonidagi asosiy tahdidlar an’anaviy "Zarar yetkazish imkoniyati × Tahdid ehtimoli" modeli asosida baholandi, xavf darajasi bo‘yicha ustuvorliklar aniqlandi. SWOT-tahlil - O‘zbekiston kiberxavfsizlik tizimining kuchli (qonuniy baza, institutsional islohotlar) va zaif tomonlari (texnik infratuzilma, mutaxassislar kamligi), imkoniyat (xalqaro hamkorlik, raqamli iqtisod) va tahdidlar (APT guruhlari, moliyaviy firibgarlik) kompleks tahlii qilindi. Statistik tahlil - Kiberhujumlar soni, yo‘qotishlar va tendensiyalar grafik, jadval va dinamik ko‘rsatkichlar shaklida sistemalashtirildi.

4. Model Yaratish Bosqichlari va Amaliy Jarayon; Taklif etilayotgan "Milliy Kiberbarqarorlik va Raqamli Suverenitet Modeli (MKRM)" quyidagi bosqichma-bosqich metodologik yondashuv asosida ishlab chiqildi:Diagnostik tahlii bosqichi - Mavjud infratuzilma, qonuniy bazaning holati, tahdidlarning migyosi va xususiyatlari aniqlandi. Xalqaro tajriba o‘rganish bosqichi - NATO, AQSh, Yevropa Ittifoqi davlatlarining kibermudofaa tizimlari, ularning samaradorlik ko‘rsatkichlari va kamchiliklari chuqur o‘rganildi. Kontekstual moslashtirish bosqichi - Xalqaro tajribalar O‘zbekistonning huquqiy, texnologik, iqtisodiy va madaniy shart-sharoitlariga moslashtirildi. Ekspert baholash bosqichi - Soha mutaxassislari,

amaliyotchi xavfsizlik mutaxassislari va huquqshunoslarning fikr-mulohazalari asosida model takomillashtirildi va amaliy joriy etish mexanizmlari ishlab chiqildi.

5. Natijalarni Baholash va Monitoring Tizimi; Model samaradorligini baholash uchun quyidagi asosiy ko‘rsatkichlar (KPI) tizimi ishlab chiqildi: Kiberhujumlar sonining nisbiy va mutlaq qisqarishi (% va birliklar hisobida) Moliyaviy firibgarliklar va ular sabab bo‘lgan iqtisodiy zararning kamayishi, Xalqaro kiberxavfsizlik indekslari (Global Cybersecurity Index) bo‘yicha o‘rning oshishi, Fuqarolarning raqamli xizmatlarga ishonch darajasi (ijtimoiy so‘rov va monitoring natijalari asosida)

6. Metodologik Cheklovlar va Istisnolar; Tadqiqotda quyidagi metodologik cheklovlar mavjudligi tan olinadi: · Ma’lumotlarning ayrim hollarda cheklanganligi va hukumat monitoring tizimlariga bog‘liqligi, Kibertahdidlarning tez o‘zgaruvchan tabiati va statistik ma’lumotlarning deyarli har oy yangilanishi, Modelning amaliy joriy etilishi uchun moliyaviy, texnik va kadrlar resurslarining mavjudligi talabi, Geosiyosiy o‘zgarishlarning kiberxavfsizlik dinamikasiga bevosita ta’siri

Ushbu metodologik yondashuv tadqiqotning ilmiy asoslanganligi, amaliy ahamiyati, natijalarning ishonchliligi va xalqaro standartlarga muvofiqligini kafolatlaydi. Har bir bosqichda tanqidiy fikrlash, kompleks tahlil va amaliy qo‘llanilishini ta’minlashga alohida e’tibor qaratildi.

Kirish

XXI asrda urush maydonlari qumloq cho'llardan va tog 'li o'rmonlardan ko'chib, ko'z bilan ko'rinmaydigan, leptonlar va baytlar olamiga aylandi. Bugun davlatlar o'rtasidagi kurash an'anaviy chegaralarni emas, balki serverlar va tarmoqlarni boshqarish uchun olib borilmoqda. Kibermakon - bu havo, quruqlik va dengiz kabi an'anaviy operatsiya maydonlariga qo'shilgan beshinchi front, u erda janglar ekranlar oldida, ovozsiz va ko'rinmas tarzda olib boriladi. Hozirgi kunda milliy xavfsizlik tushunchasi tubdan o'zgargan. Davlatlar endi nafaqat jismoniy chegaralarini, balki virtual hududlarini ham qo'riqlashlari kerak. Bir davlatning energiya tizimini butunlay o'chirib qo'yish, moliyaviy infratuzilmani buzish yoki saylov natijalariga ta'sir o'tkazish - bularning barchasi artilleriya zarbalarisiz amalga oshirilishi mumkin. Aynan shu nuqtai nazardan, kiberurushlar zamonaviy geosiyosatning eng kuchli quroliga aylangan. Ushbu maqolada biz kiberurushlarning evolyutsiyasini, ularning milliy xavfsizlikka ta'sirini va dunyoning turli mintaqalarida sodir bo'lgan real voqealar orqali bu yangi xavfning haqiqiy tabiatini o'rganamiz. Shuningdek, mamlakatimizdagi kiberxavfsizlik sohasidagi islohotlar ko‘rib chiqilib, mavjud muammolar tahlil qilinadi. Nihoyasida,

tizimlashtirilgan himoya modeli taklif etiladi. Tadqiqot quyidagi savollar asosida shakllantirildi; *global kiberxavfsizlik sohasidagi islohotlarning bosh sababi nima? O'zbekiston va Jahon miqiyosida olib borilayotgan islohotlarga qarama, qanday muammolar saqlanib qolmoqda hamda ularning yechimi nima?*

APT Guruhlari: Raqamli Jangchilar

Zamonaviy kiberurushlarning asosiy quroli - APT (Advanced Persistent Threat) guruhlaridir. Bu davlatlar tomonidan moliyalashtiriladigan, cheksiz byudjet va yuqori malakali mutaxassislardan tashkil topgan maxsus tashkilotlardir. Ularning vazifasi - dushman infratuzilmasiga uzoq muddatli kirishni ta'minlash va ma'lumotlarni to'plash. Dunyoning eng taniqli APT guruhlari orasida Rossiyaning APT29 (Cozy Bear), Xitoyning APT1 va Eronning APT34 guruhlari alohida o'rin tutadi[1]. Har biri o'ziga xos uslub va taktikaga ega bo'lib, aniq maqsadlarga qaratilgan[2].

Tarixda kiberurushlarning bir qancha hal qiluvchi voqealari ro'y bergan. Ulardan eng mashhuri - 2010-yilda Iranga qarshi Stuxnet hujumi bo'lib, u birinchi marta kiberhujumning jismoniy ob'ektlarni buzishi mumkinligini isbotladi. Bu virus Natanz yadroviy markazidagi sentrifugalarni nazorat qilib, ularni asta-sekin vayron qilgan[3]. 2020-yildagi SolarWinds hujumi esa butun dunyoni larzaga keltirdi. Rossiya razvedkasiga aloqador deb hisoblangan APT29 guruhi AQShning 18,000 dan ortiq tashkilotiga kirish huquqini qo'lga kiritdi, jumladan, Mudofaa vazirligi, Davlat departamenti va NASA kabi muhim idoralar ham ta'sirlandi[4]. Ukraina esa kiberurushlarning sinov maydoniga aylangan. 2015-yildan boshlab muntazam ravishda energiya tizimiga hujumlar, 2017-yilda NotPetya ransomware hujumi va 2022-yilda urush boshlanishi bilan birga keng ko'lamli kiberhujumlar amalga oshirildi[5].

F-35 va yangi kiberxavfsizlik davri

[1] Mandiant. APT1: Exposing One of China's Cyber Espionage Units. February 2013. Accessed November 7, 2025. https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units.

[2] Cybersecurity and Infrastructure Security Agency (CISA). "SVR Cyber Actors Adapt Tactics for Initial Cloud Access." February 26, 2024. Accessed November 7, 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a.

[3] Ralph Langner, "Iran: Computer Malware Sabotaged Uranium Centrifuges," Wired, November 29, 2010, accessed November 7, 2025, https://www.wired.com/2010/11/stuxnet-sabotage-centrifuges/.

[4] Geoff Brumfiel, "Suspected Russian hackers spied on US federal agencies," The Guardian, December 14, 2020, accessed November 7, 2025, https://www.theguardian.com/world/2020/dec/14/suspected-russian-hackers-spied-on-us-federal-agencies.

[5] U.S. Cybersecurity & Infrastructure Security Agency (CISA), "Cyber-Attack Against Ukrainian Critical Infrastructure: Alert (IR-ALERT-H-16-056-01)," accessed November 7, 2025, https://www.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01.

Kiberurushlar uch asosiy yo'nalishda olib boriladi: ma'lumot olish operatsiyalari, sabotaj va bezovtalik, dezinformatsiya kampaniyalari. Birinchi guruh intellektual mulk va harbiy sirlarni o'g'irlashni, ikkinchi guruh energetika va moliyaviy tizimlarni buzishni, uchinchi guruh esa jamoat fikrini manipulyatsiya qilishni o'z ichiga oladi.

Har uch yo‘nalish ham yuqori darajada xavfli hisoblanadi. Birinchi o‘rinda biz **ma’lumot olish operatsiyalarining** global ahamiyatini tahlil qilamiz. Bunga yaqqol misol qilib F-35 voqeasini keltirishimiz mumkin. 2010-yillarning boshida AQSh Mudofaa vazirligi va Lockheed Martin kompaniyasida ishlanayotgan eng zamonaviy F-35 Lightning II qiruvchi samolyoti loyihasi xavf ostida qolganini hech kim tasavvur ham qila olmagan edi. Bu hodisa zamonaviy kiberurushlarning haqiqiy tabiatini ochib beradigan, tarixdagi eng katta harbiy texnologik o'g'irlik epizodiga aylandi[6]. Hikoya 2010-yilda boshlangan, Xitoy razvedka xizmatiga aloqador "APT31" (Zirconium) guruhi Lockheed Martin xodimlariga ish qidirish mavzusida soxta elektron xatlar yuborganida. Bir xodim virusli ilovani yuklab olgach, guruh kompaniyaning tizimlariga kirishga muvaffaq bo'ldi. Hakerlar tizimda dastlab 9 oy davomida aniqlandi, bu vaqt davomida ular F-35 ning eng muhim sirlarini o'g'irlashga muvaffaq bo'lishdi. Dizayn chizmalari, radar tizimi spesifikatsiyalari, motor texnologiyalari va elektron urush tizimlari. Ma'lumotlar shifrlangan fayllar orqali Xitoyga yuborildi, hakerlar esa izlarni yo'q qilish uchun maxsus dasturlardan foydalandi. O'g'irlik natijasida Xitay o'zining Chengdu J-20 qiruvchi samolyotini ishlab chiqishni sezilarli darajada tezlashtirdi. Mutaxassislarning ta'kidlashicha, J-20 ning dizayni F-35 ga juda o'xshash bo'lib qoldi, bu esa to'g'ridan-to'g'ri o'g'irlangan texnologiyalarning qo'llanilishini ko'rsatadi[7]. AQSh mudofaa tizimi esa jiddiy zarar ko'rdi: 1.1 trillion dollarlik loyiha xavf ostida qoldi[8], 55 milliard dollar tadqiqot va ishlanhtirish xarajatlari va milliardlab dollar potensial eksport daromadi yo'qolish xavfi paydo bo'ldi[9]. AQSh siyosiy elitasida bu hodisani "tarixdagi eng katta harbiy texnologik

[6] Reuters. “Joint Strike Fighter plans stolen in Australia cyber attack.” Reuters, October 11, 2017. Accessed November 7, 2025. https://www.reuters.com/article/technology/joint-strike-fighter-plans-stolen-in-australia-cyber-attack-idUSKBN1CH008.

[7] Asian Times. “PLA’s J-20 fighters use stolen US tech: report.” Asia Times, October 21, 2019. Accessed November 7, 2025. https://asiatimes.com/2019/10/plas-j-20-fighters-use-stolen-us-tech-report/.

[8] U.S. Government Accountability Office (GAO), F-35 Sustainment: Costs Continue to Rise While Planned Actions Could Reduce Some Long-Term Costs, GAO-24-106703, April 15, 2024, accessed November 7, 2025, https://www.gao.gov/products/gao-24-106703.

[9] Jeffrey Gertler, F-35 Joint Strike Fighter (JSF) Program: Background, Status, and Issues, Congressional Research Service report RL30563, February 16, 2012, accessed November 7, 2025, https://www.everycrsreport.com/files/20120216_RL30563_d64afecc9e8d4b2069afb19013104a4bb7de5eec.pdf.

o'g'irlik" deya tanqidiy baholandi[10]. Bu hodisa butun NATO ittifoqining kiberxavfsizlik strategiyasini o'zgartirishga majbur qildi. AQSh esa mudofaa kontraktorlari uchun yangi xavfsizlik standartlarini joriy qilishga to'g'ri keldi. Eng xavfli jihati - bu hujumlarning keng ko'lamli iqtisodiy oqibatlaridir. 2015-yilda global iqtisodiyot intellektual mulk o'g'irligidan 300 milliard dollar zarar ko'rgan bo'lsa, 2023-yilga kelib bu ko'rsatkich bir necha milliard dollarga oshdi[11]. Intellektual mulkning yo'qolishi, kompaniyalarning obro'siga putur yetishi va investitsiyalarning qisqarishi - bularning hammasi milliy xavfsizlikka bevosita tahdiddir.

Biroq bu voqea yuqorida aytilganidek, kiber xavfsizlik sohasida bir qancha yangi islohotlarni o‘tkazlishiga turtki bo‘ldi. Xususan, "Zero Trust" arxitekturasining qo‘llanilishi ishonchsizlik konsepsiyasi bilan kiber mudofaani yangi bosqichga olib chiqdi. Ko'p bosqichli autentifikatsiya tizimlari, doimiy monitoring, xodimlarni muntazam o'qitish dasturlari ham bu bosqichning davomiyligini ta’minladi[12].

O‘zbekistonda kiberxavfsizlik sohasida amalga oshirilayotgan islohotlar

So‘nggi yillarda dunyo miqyosida raqamli infratuzilma tez sur’atlarda rivojlanar ekan, axborot tizimlariga nisbatan kiberhujumlar soni ham keskin ortib bormoqda. Xususan, xalqaro miqyosdagi yirik harbiy va texnologik hodisalar, jumladan, F-35 dasturi bilan bog‘liq kiberxavfsizlik mojarolari ko‘plab davlatlarni, jumladan O‘zbekistonni ham o‘z axborot makonini himoya qilish choralarini kuchaytirishga undadi. Shu bois, mamlakatda kiberxavfsizlikni milliy xavfsizlik tizimining ustuvor yo‘nalishlaridan biri sifatida rivojlantirishga qaratilgan qator islohotlar amalga oshirilmoqda. Avvalo, 2022-yilda “Kiberxavfsizlik to‘g‘risida”gi Qonun qabul qilinishi bu sohada tub burilish yasadi. Mazkur hujjat axborot infratuzilmasining barqarorligini ta’minlash, davlat organlari, bank-moliya tizimi, energetika, transport va boshqa strategik tarmoqlarning raqamli himoyasini mustahkamlashni nazarda tutadi. Qonunga muvofiq, endilikda kiberxavfsizlik faqat texnik masala emas, balki mamlakat suvereniteti va iqtisodiy barqarorligining ajralmas qismi sifatida qaralmoqda[13]. Shuningdek, 2024-yilda

[10] Derek S. Reveron and John R. Deni (eds.), Confronting China’s Efforts to Steal Defense Information, Belfer Center, May 4, 2020, accessed November 7, 2025, https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information.

[11] World Intellectual Property Organization, IP Facts and Figures 2023 (Geneva: WIPO, 2023), accessed November 7, 2025, https://www.wipo.int/edocs/pubdocs/en/wipo%E2%80%91pub%E2%80%91943%E2%80%912023%E2%80%91en%E2%80%91wipo%E2%80%91ip%E2%80%91facts%E2%80%91and%E2%80%91figures%E2%80%912023.pdf

[12] National Institute of Standards and Technology, Zero Trust Architecture, Special Publication 800-207 (Gaithersburg, MD: NIST, August 2020), accessed November 7, 2025, https://www.nist.gov/publications/zero-trust-architecture.

[13] O‘zbekiston Respublikasi Oliy Majlisi Qonunchilik palatasi, “Kiberxavfsizlik to‘g‘risida”gi Qonun, O‘RQ-764-son, 15 aprel 2022, accessed November 7, 2025, https://lex.uz/docs/-5960604.

O‘zbekiston Respublikasi Senati bank va moliyaviy tizimlarda kiberxavfsizlikni ta’minlashga doir qonunchilikni takomillashtirishga oid o‘zgartirishlarni ma’qulladi. Ushbu o‘zgarishlar orqali Markaziy bankka kiberxavfsizlik bo‘yicha qo‘shimcha vakolatlar berildi hamda to‘lov tizimlari, kredit tashkilotlari va elektron moliya infratuzilmalari uchun yangi xavfsizlik standartlari belgilandi[14]. Bu o‘zgarishlar moliyaviy sohadagi kiberjinoyatlar xavfini kamaytirishga xizmat qilmoqda. Keyingi muhim qadam sifatida, 2025-yil 30-aprel kuni Prezident farmoni bilan “Axborot texnologiyalari orqali sodir etiladigan jinoyatlarga qarshi kurashni kuchaytirish chora-tadbirlari to‘g‘risida”gi qaror qabul qilindi. Unga ko‘ra, bank kartalari, SIM-kartalar, elektron hamyonlar va mobil to‘lov tizimlaridan noqonuniy foydalanish holatlariga qarshi kurash tizimi takomillashtirildi. Endilikda ushbu vositalar jinoyatlarda ishlatilsa, nafaqat shaxs, balki tashkilotlar ham javobgarlikka tortilishi belgilandi. Bu esa mamlakatda kiberjinoyatchilikning oldini olishda muhim bosqich bo‘ldi[15]. Davlat infratuzilmasi doirasida ham muhim tashkiliy choralar ko‘rildi. UZINFOCOM kompaniyasi va Raqamli texnologiyalar vazirligi hamkorligida “UZSOC” – Axborot xavfsizligi markazi tashkil etilib, 24 soatlik monitoring va tezkor javob berish tizimi yo‘lga qo‘yildi. Mazkur markaz davlat idoralari va muhim axborot infratuzilmasining kiberholatini doimiy kuzatish, tahdidlarni aniqlash hamda ularning oqibatlarini bartaraf etish bilan shug‘ullanadi. Bundan tashqari, O‘zbekiston Xalqaro hamjamiyat bilan hamkorlikni kengaytirgan holda, Yevropada xavfsizlik va hamkorlik tashkiloti (OSCE) bilan birgalikda davlat xizmatchilari uchun kiberxavfsizlik bo‘yicha o‘quv-trening dasturlarini amalga oshirmoqda[16]. Bu esa milliy mutaxassislar salohiyatini oshirish, tajriba almashish va xalqaro standartlarga moslashish imkonini bermoqda. Natijada, O‘zbekistonning xalqaro nufuzida ham ijobiy o‘zgarishlar kuzatildi. Xususan, 2024-yilgi “Global Cybersecurity Index” reytingida mamlakat “faol rivojlanayotgan kiberxavfsizlik tizimiga ega davlatlar” qatoriga kiritildi. Bu natija so‘nggi yillarda olib borilgan islohotlarning samaradorligini ko‘rsatadi[17].

[14] O‘zbekiston Respublikasi Oliy Majlisi Qonunchilik palatasi, “Kiberxavfsizlikni ta’minlash sohasidagi …”gi Qonun, O‘RQ-964-son, 20 sentabr 2024, accessed November 7, 2025, https://lex.uz/uz/docs/-7108720.

[15] O‘zbekiston Respublikasi Prezidentining, “Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida”gi PQ-153-son qaror, 30 aprel 2025, accessed November 7, 2025, https://lex.uz/ru/docs/-7511145.

[16] “Launch of UZSOC: Cyber Threat Monitoring and Management System”, UZINFOCOM (Toshkent: 2 Avgust 2024), accessed November 7 2025, https://uzinfocom.uz/en/projects/uzsoc-ru-29.

[17] International Telecommunication Union, Global Cybersecurity Index 2024 (GCI 5th Edition) (Geneva: ITU, September 12, 2024), accessed November 7, 2025, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf.

Raqamli transformatsiya — hukumat xizmatlarining onlaynga o‘tkazilishi, elektron to‘lovlar hajmining oshishi va biznesning raqamlashuvi — O‘zbekiston iqtisodiy va ijtimoiy hayotini tubdan o‘zgartirmoqda. Biroq bu yutuqlar bilan birgalikda mamlakat kiberxavfsizligida sezilarli muammolar yuzaga chiqmoqda. Quyida eng muhim uch muammo, ularning amaliy tasviri va mamlakat miqyosidagi kuchli statistik dalillari keltiriladi.

1) Kiberhujumlarning keskin ko‘payishi: keng miqyosli xatarlar

Muammo: davlat va xususiy sektor tizimlariga qaratilgan kiberhujumlar tez sur’atda ortmoqda; himoyalanish darajasi esa ko‘pincha talab darajasida emas.

Hayotiy statistika: 2024 yilda mamlakat bo‘yicha 12 milliondan ortiq kiberhujum qayd etilgan[18]; qisman ma’lumotlar so‘nggi besh yilda kiberjinoyatlar soni 68 baravarga oshganini ko‘rsatadi[19]. Bu xatarlar qatorida veb-resurslarga, davlat xizmatlarining portallariga va onlayn xizmatlarga qaratilgan masshtabli bot-hujumlar mavjud.

Tahlil: ko‘payib borayotgan xurujlar ikki omil bilan bog‘liq: birinchidan, raqamli xizmatlar kengroq qamrov oldi; ikkinchidan, tizimlardagi zaifliklar hamon mavjud. Natijada xizmatlar uzilishi, ma’lumotlar o‘g‘irlanishi va obro‘ga zarar yetishi kabi oqibatlar yuz beradi.

2) Moliyaviy firibgarliklar va kiberjinoyatlar: fuqarolar hamda iqtisodga bevosita zarar

Muammo: kiberjinoyatlar, xususan bank kartalari va elektron to‘lovlar orqali amalga oshiriladigan firibgarliklar ustunlik qilmoqda; buning oqibatida fuqarolar zarar ko‘rmoqda va moliyaviy ishonch pasaymoqda.

Hayotiy statistika: kiberjinoyatlar ichida bank-kartalarga oid firibgarliklar eng ko‘p tarqalgan — kiberjinoyatlar umumiy jinoyatlar tarkibida sezilarli ulushga ega bo‘lib,

[18] Cybersecurity Centre of the Republic of Uzbekistan, “Over 12 million cyber-attack attempts in Uzbekistan in 2024,” AKIpress News Agency, February 4, 2025, accessed November 7, 2025, https://www.akipress.com/news/817364.html.

[19] Gazeta.uz, “Cybercrimes in Uzbekistan increase 68-fold in five years,” May 31, 2025, accessed November 7, 2025, https://www.gazeta.uz/en/2025/05/31/cybercrime/

2024 yilda ularning qismi keskin oshdi. So‘nggi yillarda kiberjinoyatlar sonining ko‘payishi bilan birgalikda iqtisodiy zarar ham sezilarli cho‘qqiga chiqdi[20].

Tahlil: bu muammo faqat texnik zaiflik emas — fuqarolarning raqamli moliyaviy xabardorligi pastligi, SMS/ phishing hujumlariga qarshi himoya yo‘qligi va moliyaviy tashkilotlardagi ayrim protseduralarning zaifligi ham rol o‘ynaydi. Natijada aholining onlayn moliyaviy xizmatlarga ishonchi zaiflashadi, bu esa raqamli iqtisodiyotning rivojlanishiga to‘siq bo‘lishi mumkin.

3) Infratuzilmadagi zaifliklar va zaifliklarni aniqlash tizimlarining yetishmasligi

Muammo: davlat domenlari, onlayn portallar va xususiy sektor tizimlarida xavfsizlik sertifikatlari yoki zamonaviy himoya choralarining yetishmasligi — umumiy xavf omilidir. Zaifliklarni aniqlash va bartaraf etish bo‘yicha milliy tizimlar to‘liq ivishmagan.

Hayotiy statistika: milliy domen segmentida (masalan, .uz) faol domenlar orasida xavfsizlik sertifikatlari va himoya vositalari bilan qamrab olingan saytlarning ulushi kutilgan darajada emas; shu bilan birga, ayrim yillarda domen segmentiga yuzlab minglab hujumlar qayd etilgan.[21]

Tahlil: zaif infratuzilma hujumlarni osonlashtiradi va shaxsiy hamda davlat ma’lumotlarining xavfsizligini zaiflashtiradi. Qo‘shni tizimlarga ketma-ket zaifliklar tarqalishi ham mumkin — masalan, yomon konfiguratsiya qilingan server orqali tarmoq ichidagi boshqa resurslarga ham zarar yetishi ehtimoli mavjud.

Milliy Kiberbarqarorlik va Raqamli Suverenitet Modeli (MKRM)

Muallif tomonidan taklif etilgan “Milliy Kiberbarqarorlik va Raqamli Suverenitet Modeli (MKRM)” — bu texnologik, iqtisodiy va ijtimoiy omillarni birlashtirgan kompleks boshqaruv tizimi bo‘lib, O‘zbekiston sharoitiga moslashtirilgan. Modelning asosiy maqsadi — davlat, biznes va fuqarolarni yagona kiberxavfsizlik mexanizmi orqali himoya qilish, kiberhujumlarning oldini olish va raqamli suverenitetni mustahkamlashdan iborat.

[20] Ministry of Internal Affairs of the Republic of Uzbekistan, “Cybercrimes in Uzbekistan rise 68-fold: Nearly 2 trillion UZS stolen in five years,” Kun.uz, May 29, 2025, accessed November 7, 2025,

[21] Sh. A. Gafurov, “Statistical Analysis of the ‘.UZ’ Domain of the Internet Network,” Conferencea (2024: 30th Tech-Fest: USA September), published September 19, 2024, accessed November 7 2025, https://conferencea.org/index.php/conferences/article/view/3515.

Model uch asosiy ustunga tayanadi:

A) Texnologik barqarorlik (Cyber Defense Core)

Bu yo‘nalish davlat va xususiy sektordagi texnik himoya tizimlarini birlashtiradi. Uning doirasida: Yagona Kiber Monitoring Markazi (YKMM) tashkil etilib, barcha tarmoqlarning real vaqtda xavfsizlik holati kuzatiladi; Sun’iy intellekt asosidagi Threat Prediction tizimi orqali kiberhujumlar sodir bo‘lishidan oldin prognozlanadi; Milliy bulut xavfsizlik platformasi yordamida davlat idoralari uchun yagona sertifikatlangan muhit yaratiladi. Bu yo‘nalish kiberhujumlarning kamayishiga va infratuzilmadagi zaifliklarni bartaraf etishga xizmat qiladi.

B) Iqtisodiy himoya va moliyaviy xavfsizlik (Cyber Economy Shield)

Bu ustun kiberjinoyatlar va moliyaviy firibgarliklarga qarshi chora-tadbirlarni o‘z ichiga oladi: Banklararo Kiber Xavfsizlik Konsorsiumi (BKXK) orqali barcha moliyaviy institutlar yagona himoya protokollaridan foydalanadi; “Antiphishing Uzbekistan” dasturi fuqarolarni onlayn firibgarliklardan himoya qiladi; Har bir moliyaviy tashkilotda yillik kiberxavfsizlik auditi majburiy etib belgilanadi. Natijada, iqtisodiy xavfsizlik mustahkamlanadi, raqamli to‘lov tizimlariga ishonch oshadi.

C) Inson kapitali va raqamli madaniyat (Cyber Literacy & Governance)

Modelning uchinchi yo‘nalishi kiberxavfsizlikning ijtimoiy asosini mustahkamlaydi: “CyberSafe Schools” dasturi orqali maktab va kollejlar tizimida axborot xavfsizligi fanlari joriy etiladi; “Digital Trust” milliy platformasi fuqarolarning raqamli identifikatsiya va shaxsiy ma’lumotlarini markazlashtirilgan tarzda himoya qiladi; Davlat xizmatchilari uchun kiberxavfsizlik bo‘yicha sertifikatsiya tizimi yo‘lga qo‘yiladi. Bu yo‘nalish inson xatolarini kamaytiradi va fuqarolarning raqamli madaniyatini oshiradi.

Ushbu modeldan quyidagicha natijalar kutiladi:

Davlat tizimlarida kiberhujumlar soni 60–70% gacha qisqaradi. Moliyaviy firibgarliklar hajmi 2–3 yil ichida 50% gacha kamayadi. Fuqarolarning raqamli xizmatlarga ishonchi oshadi, natijada raqamli iqtisodiyot ulushi YAIMning 15–20% gacha yetadi. O‘zbekiston Markaziy Osiyoda kiberbarqarorlik indeksi bo‘yicha yetakchi davlatga aylanishi mumkin.

O‘zbekiston uchun kiberxavfsizlikni ta’minlash endilikda faqat texnik chora-tadbirlar majmuasi emas, balki milliy xavfsizlik strategiyasining tarkibiy qismiga aylanishi

zarur. Taklif etilgan "Milliy Kiberbarqarorlik va Raqamli Suverenitet Modeli" texnologik himoya, iqtisodiy barqarorlik va inson omilini birlashtirib, mamlakatni raqamli davrda mustahkam, xavfsiz va suveren davlat sifatida rivojlantirishga xizmat qiladi. Bu modelning joriy etilishi O'zbekistonni nafaqat kiberhujumlar va firibgarliklarga qarshi himoyalaydi, balki uni mintaqadagi raqamli siyosiy mustaqillik va kiberbarqarorlik markaziga aylantirish imkonini beradi.

BIBLIOGRAPHY

1. Mandiant. APT1: Exposing One of China's Cyber Espionage Units. February 2013. Accessed November 7, 2025. https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units.
2. Cybersecurity and Infrastructure Security Agency (CISA). "SVR Cyber Actors Adapt Tactics for Initial Cloud Access." February 26, 2024. Accessed November 7, 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a.
3. Ralph Langner, "Iran: Computer Malware Sabotaged Uranium Centrifuges," Wired, November 29, 2010, accessed November 7, 2025, https://www.wired.com/2010/11/stuxnet-sabotage-centrifuges/.
4. Geoff Brumfiel, "Suspected Russian hackers spied on US federal agencies," The Guardian, December 14, 2020, accessed November 7, 2025, https://www.theguardian.com/world/2020/dec/14/suspected-russian-hackers-spied-on-us-federal-agencies.
5. U.S. Cybersecurity & Infrastructure Security Agency (CISA), "Cyber-Attack Against Ukrainian Critical Infrastructure: Alert (IR-ALERT-H-16-056-01)," accessed November 7, 2025, https://www.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01.
6. Reuters. "Joint Strike Fighter plans stolen in Australia cyber attack." Reuters, October 11, 2017. Accessed November 7, 2025. https://www.reuters.com/article/technology/joint-strike-fighter-plans-stolen-in-australia-cyber-attack-idUSKBN1CH008.
7. Asian Times. "PLA's J-20 fighters use stolen US tech: report." Asia Times, October 21, 2019. Accessed November 7, 2025. https://asiatimes.com/2019/10/plas-j-20-fighters-use-stolen-us-tech-report/.
8. U.S. Government Accountability Office (GAO), F-35 Sustainment: Costs Continue to Rise While Planned Actions Could Reduce Some Long-Term Costs, GAO-24-106703, April 15, 2024, accessed November 7, 2025, https://www.gao.gov/products/gao-24-106703.

9. Jeffrey Gertler, F-35 Joint Strike Fighter (JSF) Program: Background, Status, and Issues, Congressional Research Service report RL30563, February 16, 2012, accessed November 7, 2025, https://www.everycrsreport.com/files/20120216_RL30563_d64afecc9e8d4b2069afb19013104a4bb7de5eec.pdf.
10. Derek S. Reveron and John R. Deni (eds.), Confronting China's Efforts to Steal Defense Information, Belfer Center, May 4, 2020, accessed November 7, 2025, https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information.
11. World Intellectual Property Organization, IP Facts and Figures 2023 (Geneva: WIPO, 2023), accessed November 7, 2025, https://www.wipo.int/edocs/pubdocs/en/wipo%E2%80%91pub%E2%80%919943%E2%80%912023%E2%80%91en%E2%80%91wipo%E2%80%91ip%E2%80%91facts%E2%80%91and%E2%80%91figures%E2%80%912023.pdf
12. National Institute of Standards and Technology, Zero Trust Architecture, Special Publication 800-207 (Gaithersburg, MD: NIST, August 2020), accessed November 7, 2025, https://www.nist.gov/publications/zero-trust-architecture.
13. O‘zbekiston Respublikasi Oliy Majlisi Qonunchilik palatasi, “Kiberxavfsizlik to‘g‘risida”gi Qonun, O‘RQ-764-son, 15 aprel 2022, accessed November 7, 2025, https://lex.uz/docs/-5960604.
14. O‘zbekiston Respublikasi Oliy Majlisi Qonunchilik palatasi, “Kiberxavfsizlikni ta’minlash sohasidagi …”gi Qonun, O‘RQ-964-son, 20 sentabr 2024, accessed November 7, 2025, https://lex.uz/uz/docs/-7108720.
15. O‘zbekiston Respublikasi Prezidentining, “Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida”gi PQ-153-son qaror, 30 aprel 2025, accessed November 7, 2025, https://lex.uz/ru/docs/-7511145
16. “Launch of UZSOC: Cyber Threat Monitoring and Management System”, UZINFOCOM (Toshkent: 2 Avgust 2024), accessed November 7 2025, https://uzinfocom.uz/en/projects/uzsoc-ru-29.
17. International Telecommunication Union, Global Cybersecurity Index 2024 (GCI 5th Edition) (Geneva: ITU, September 12, 2024), accessed November 7, 2025, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf.

18. Cybersecurity Centre of the Republic of Uzbekistan, "Over 12 million cyber-attack attempts in Uzbekistan in 2024," AKIpress News Agency, February 4, 2025, accessed November 7, 2025, https://www.akipress.com/news/817364.html.
19. Gazeta.uz, "Cybercrimes in Uzbekistan increase 68-fold in five years," May 31, 2025, accessed November 7, 2025, https://www.gazeta.uz/en/2025/05/31/cybercrime/
20. Ministry of Internal Affairs of the Republic of Uzbekistan, "Cybercrimes in Uzbekistan rise 68-fold: Nearly 2 trillion UZS stolen in five years," Kun.uz, May 29, 2025, accessed November 7, 2025,
21. Sh. A. Gafurov, "Statistical Analysis of the '.UZ' Domain of the Internet Network," Conferencea (2024: 30th Tech-Fest: USA September), published September 19, 2024, accessed November 7 2025, https://conferencea.org/index.php/conferences/article/view/3515