RAQAMLI ASR TAHDIDLARI: KIBERJINOYATCHILIKNING ZAMONAVIY KO'RINISHLARI.

Raxmatov Bobur To‘lqin o‘g‘li
O‘zbekiston Respublikasi IIV Akademiyasi Jinoyat huquqi kafedrasi o‘qituvchisi, kapitan
Ergashov Ro‘zimuhammad Akmal o‘g‘li
O‘zbekiston Respublikasi IIV Akademiyasi
131-guruh kursanti, safdor
https://doi.org/10.5281/zenodo.18876656

ARTICLE INFO

Qabul qilindi: 24-fevral 2026 yil
Ma’qullandi: 26- fevral 2026 yil
Nashr qilindi: 28-fevral 2026 yil

KEYWORDS

Kiberjinoyat, axborot xavfsizligi, ijtimoiy muhandislik, fishing, ransomware (tovlamachi dasturlar), raqamli gigiena, sun’iy intellekt, O‘zbekiston qonunchiligi.

ABSTRACT

Ushbu maqola XXI asrning eng dolzarb muammolaridan biri - kiberjinoyatchilik va uning jamiyatga ta’sirini tahlil qilishga bag‘ishlangan. Maqolada kiberjinoyat turlari, ularning evolyutsiyasi, xususan, fishing, ijtimoiy muhandislik va sun’iy intellekt yordamida amalga oshirilayotgan yangi tahdidlar o‘rganilgan. O‘zbekiston Respublikasining axborot xavfsizligi sohasidagi qonunchiligi va xalqaro tajriba (AQSh, Yevropa Ittifoqi) qiyosiy tahlil qilingan. Tadqiqot natijasida raqamli savodxonlikni oshirish va texnik himoya vositalarining integratsiyasi jinoyatchilikni kamaytirishning asosiy omili ekanligi asoslab berilgan.

Bugungi kunda biz "To‘rtinchi sanoat inqilobi" davrida yashayapmiz. Internet va raqamli texnologiyalar hayotimizning ajralmas qismiga aylandi. Ertalab uyg‘onishimizdan to uxlashimizgacha bo‘lgan jarayonda smartfonlar, bank ilovalari, ijtimoiy tarmoqlar va bulutli xizmatlardan foydalanamiz. "Raqamli O‘zbekiston – 2030" strategiyasi doirasida mamlakatimizda ham davlat xizmatlari va iqtisodiyot jadal raqamlashtirilmoqda. Biroq, texnologik taraqqiyot o‘zining "qora tomoni"ni ham namoyon etmoqda: bulardan asosiy biri kiberjinoyatchilikdir.

Raqamlashgan hayotimizda atrofimga nazar tashlasak, deyarli har kuni kimdir Telegram orqali "soxta havola"ga kirib qo‘ygani yoki bank kartasidan pul yechib olingani haqida eshitamiz. Agar avvallari jinoyatchilar bankka qurol bilan bostirib kirishgan bo‘lsa, bugungi kunda ular uyda, qulay kresloda o‘tirib, bir necha tugmani bosish orqali millionlab dollarlarni o‘zlashtirmoqda.

Ushbu maqolaning maqsadi – kiberjinoyatchilikning shunchaki "xakerlik" emas, balki murakkab psixologik va texnik jarayon ekanligini ochib berish, uning zamonaviy turlarini tasniflash va unga qarshi kurashishda yoshlar (talabalar) va davlat qanday hamkorlik qilishi kerakligini tahlil qilishdir. Bizning oldimizda turgan asosiy savol: "Texnologiya rivojlangani sari biz xavfsizroq bo‘lyapmizmi yoki aksincha?"

Tadqiqot materiallari va metodologiyasi (Materials and Methods)

Ushbu maqolani yozishda mavzuni chuqur o‘rganish uchun tavsifiy tahlil (descriptive analysis) va qiyosiy-huquqiy (comparative-legal) metodlardan foydalanildi.

Foydalanilgan manbalar:

1.O‘zbekiston qonunchiligi: O‘zbekiston Respublikasining "Kiberxavfsizlik to‘g‘risida"gi Qonuni va Jinoyat Kodeksining tegishli moddalari (masalan, 168-modda – Firibgarlik, axborot texnologiyalaridan foydalanib).

2.Xalqaro hisobotlar: "Interpol", "Kaspersky Lab" va "Group-IB" kabi xalqaro kiberxavfsizlik tashkilotlarining yillik hisobotlari.

3.Ilmiy adabiyotlar: Axborot xavfsizligi bo‘yicha mahalliy va xorijiy olimlarning ilmiy maqolalari.

4.Statistik ma’lumotlar: O‘zbekiston IIV Kiberxavfsizlik markazi tomonidan e’lon qilingan ochiq ma’lumotlar.

Tadqiqot jarayonida kiberjinoyatlarni faqat texnik hodisa sifatida emas, balki ijtimoiy-psixologik fenomen sifatida o‘rganishga harakat qilindi. Chunki statistikaga ko‘ra, kiberhujumlarning 90% dan ortig‘i inson omili (xato yoki ishonuvchanlik) tufayli sodir bo‘ladi.

Muhokama va natijalar (Results and Discussion)

Raqamli texnologiyalar rivojlanishi bilan insoniyat yangi bir makon — kiberfazoga ko‘chdi. Biroq, har qanday sivilizatsiya kabi, bu makon ham o‘zining qorong‘u tomonlariga ega. Ilmiy nuqtayi nazardan qaraganda, **kiberjinoyat** — bu shunchaki kompyuter orqali qilingan qilmish emas, balki kiberfazoning o‘ziga xos xususiyatlaridan foydalanib sodir etiladigan murakkab ijtimoiy-huquqiy hodisadir. Xalqaro huquq, xususan, Budapesht konvensiyasi kiberjinoyatni kompyuter tizimlari va ma’lumotlarining maxfiyligi, butunligi va foydalana olish imkoniyatiga qarshi qaratilgan har qanday noqonuniy harakat sifatida tasniflaydi. Bu yerda kompyuter ham jinoyatning **quroli** (masalan, hujum uyushtirish uchun), ham uning **ob’ekti** (ma’lumotlarni o‘g‘irlash uchun) vazifasini o‘taydi.

Ushbu tahdidlarga qarshi turuvchi kuch esa **kiberxavfsizlik** deb ataladi. ISO/IEC 27032 xalqaro standarti kiberxavfsizlikka kiberfazodagi aktivlarni, ya’ni bizning shaxsiy ma’lumotlarimizdan tortib davlat ahamiyatiga molik infratuzilmalargacha bo‘lgan boyliklarni himoya qilish jarayoni sifatida qaraydi. Kiberxavfsizlikning fundamental asosi jahon ilm-fanida **"CIA triadasi"** (Maxfiylik, Butunlik va Foydalana olishlik) tushunchasi bilan bog‘lanadi. Ya’ni, xavfsizlik mutaxassislarining asosiy vazifasi ma’lumotni begonadan yashirish (Maxfiylik), uni o‘zgarishsiz saqlash (Butunlik) va kerakli vaqtda unga yo‘l ochib berishni (Foydalana olishlik) ta’minlashdir.

Ushbu ikki tushuncha o‘rtasidagi bog‘liqlikni **"doimiy evolyutsion zanjir"** deb atash mumkin. Ularni bir-birisiz tasavvur qilish imkonsiz: kiberjinoyat "kasallik" bo‘lsa, kiberxavfsizlik uning "vaksina"sidir. Bu jarayon xuddi biologik evolyutsiyaga o‘xshaydi — viruslar mutatsiya bo‘lib, murakkablashgani sari, inson organizmi (ya’ni kiberxavfsizlik tizimlari) yanada kuchliroq immunitet hosil qilishga majbur bo‘ladi. Masalan, kiberjinoyatchilar sun’iy intellektdan foydalanib murakkab fishing hujumlarini (kiberjinoyat) uyushtira boshlagach, kiberxavfsizlik sohasi ham javob tariqasida intellektual monitoring tizimlarini yaratdi.

Binobarin, kiberxavfsizlik kiberjinoyatchilikning mavjudligi tufayli doimiy harakatda bo‘lgan dinamik jarayondir. Agar kiberjinoyat raqamli tartibni buzishga qaratilgan entropiya (tartibsizlik) bo‘lsa, kiberxavfsizlik — bu tartibni qayta tiklovchi va barqarorlikni ta’minlovchi kuchdir. O‘zbekiston sharoitida ushbu ikki qutbning kurashi nafaqat texnik vositalar, balki huquqiy normalar va raqamli madaniyat orqali muvozanatga

keltirilmoqda. Xulosa qilib aytganda, kiberjinoyat va kiberxavfsizlik — bu raqamli taraqqiyotning ajralmas ikki tomoni bo‘lib, birining rivojlanishi ikkinchisining takomillashishini taqozo etadi.

Kiberjinoyatchilik olami juda keng va u doimiy o‘zgarib turadi. Tahlillarim natijasida zamonaviy kiberjinoyatlarni quyidagi asosiy toifalarga bo‘lib o‘rganish kera

Ijtimoiy muhandislik (Social Engineering) – Eng xavfli qurol

Ko‘pchilik kiberjinoyatchini murakkab kodlar yozayotgan daho dasturchi deb tasavvur qiladi. Ko‘pchilik kiberjinoyatchini qora ko'zoynak taqqan, zulmatda murakkab kodlar yozayotgan daho dasturchi deb tasavvur qiladi. Biroq, zamonaviy kiber-psixologiya shuni ko'rsatadiki, eng xavfli hujumlar texnik kodlar bilan emas, balki inson his-tuyg'ulari bilan amalga oshiriladi. **Ijtimoiy muhandislik** — bu inson psixologiyasini manipulyatsiya qilish orqali uning e’tiborini chalg‘itish va ixtiyoriy ravishda maxfiy ma’lumotlarni topshirishga majbur qilish san’atidir[1]. Bu jarayonda jinoyatchi dasturiy ta'minotdagi xatoni emas, balki inson tabiatidagi ishonuvchanlik, qo‘rquv yoki qiziquvchanlik kabi "psixologik bo'shliq"larni qidiradi.

Ushbu sohaning eng "ommabop" va yashirin usuli — **Fishing (Phishing)** hisoblanadi. Fishing — bu raqamli dunyodagi "qarmoq"dir. Bugungi kunda O‘zbekiston kiber-fazosida "Click" yoki "Payme" to‘lov tizimlari nomidan yuborilayotgan "Karta bloklandi" yoki "Siz kutilmagan yutuq sohibi bo‘ldingiz" kabi soxta SMS xabarlar aynan shu "qarmoq"ning bir ko‘rinishidir. Ayniqsa, talabalar orasida Telegram platformasi orqali keng tarqalayotgan "Prezident qarori bilan barcha talabalarga moddiy yordam berilmoqda" qabilidagi feyk xabarlar jamiyatning ijtimoiy ehtiyojlaridan ustalik bilan foydalanishni ko‘rsatadi. Foydalanuvchi o‘ziga ko‘rsatilgan soxta, lekin tashqi ko‘rinishidan rasmiy saytdan deyarli farq qilmaydigan havolaga kirib, karta ma’lumotlarini kiritar ekan, u o‘z qo‘li bilan "raqamli hamyoni" kalitini jinoyatchiga topshirib qo‘yganini sezmay ham qoladi.

Ijtimoiy muhandislikning yanada "jonli" ko'rinishi — bu **Vishing (Voice Phishing)**, ya'ni telefon orqali amalga oshiriladigan psixologik hujumdir. Bunda firibgar o‘zini "Bank xavfsizlik xizmati xodimi" yoki "Huquq-tartibot organi vakili" sifatida tanishtirib, go‘yoki foydalanuvchi hisobida shubhali operatsiya sodir bo‘layotganini ma’lum qiladi. Bu yerda **"nufuz effekti" (authority bias)** ishga tushadi: inson rasmiy tashkilot nomini eshitganda, tanqidiy fikrlashni to‘xtatib, qarshi tomonga to‘liq bo‘ysunishni boshlaydi. Jinoyatchi tomonidan so‘ralgan oddiygina "tasdiqlash kodi" (SMS kod) aslida sizning pullaringizni yechib olish uchun yakuniy ruxsatnoma bo‘lib xizmat qiladi.

Tovlamachi dasturlar (Ransomware)

Agar ijtimoiy muhandislikni "aldov yo‘li bilan kirish" deb ta’riflasak, **tovlamachi dasturlarni (Ransomware)** zamonaviy raqamli olamning "qurolli bosqinchiligi" yoki "kiber-o‘g‘riligi" deb atash mumkin. Bu shunchaki kompyuter tizimidagi nosozlik emas, balki axborotni garovga olish orqali amalga oshiriladigan yuqori texnologik shantajdir.

Murakkabroq yondashsak, tovlamachi dasturlar — bu foydalanuvchining ma’lumotlarini **asimetrik shifrlash** algoritmlari yordamida o‘qib bo‘lmaydigan holatga keltiruvchi zararli kodlardir. Jinoyatchilar tizimga suqulib kirgach, barcha hayotiy muhim fayllarni (hujjatlar, ma’lumotlar bazalari, shaxsiy arxivlar) "qulflab" qo‘yishadi. Shundan so‘ng, ekranda psixologik

[1] Hadnagy, C. *Social Engineering: The Science of Human Hacking*. 2nd Edition, Wiley, 2018. Ushbu manbada ijtimoiy muhandislik texnik vositalardan ko‘ra ko‘proq inson omiliga asoslangan kiber-hujum ekanligi ilmiy isbotlangan.

bosimga asoslangan xabarnoma paydo bo‘ladi: "Fayllaringiz shifrlangan. Ularni qayta tiklash (dekriptsiya) uchun 24-48 soat ichida ma’lum miqdorda (odatda 1000$ dan bir necha million dollargacha) mablag‘ni kriptovalyutada (Bitcoin yoki Monero) o‘tkazing". Kriptovalyutaning tanlanishi tasodif emas — bu tranzaksiyalarning anonimligini ta’minlaydi va jinoyat izini virtual fazoda yo‘qotib yuboradi

Global tahlil: Tovlamachi dasturlarning xavfliligi shundaki, ular nafaqat shaxsiy kompyuterlarni, balki butun boshli davlat infratuzilmalarini falaj qilish quvvatiga ega.

Bunga yaqqol misol sifatida 2017-yilda sodir bo‘lgan **"WannaCry"** pandemiyasini keltirish mumkin. Ushbu virus dunyoning 150 dan ortiq mamlakatidagi 200 mingdan ziyod kompyuterlarni zararladi. Eng dahshatlisi, Buyuk Britaniyadagi Milliy sog‘liqni saqlash tizimi (NHS) hujumga uchragani sababli minglab jarrohlik amaliyotlari bekor qilindi, shifoxonalar bemorlarni qabul qila olmay qoldi. Bu voqea kiberxavfsizlik tarixida burilish nuqtasi bo‘ldi: biz "bitta virus butun jamiyat hayotini to‘xtatib qo‘yishi mumkin" degan achchiq haqiqat bilan yuzlashdik[2].

Bugungi kunda tovlamachi dasturlar yanada takomillashib, **"Ransomware-as-a-Service" (RaaS)** ko‘rinishiga keldi. Endilikda jinoyatchi bo‘lish uchun professional dasturchi bo‘lish shart emas — zararli dasturni "ijaraga olib", tayyor biznes-model sifatida foydalanish mumkin. Bu esa kiber-tahdidlar ko'lamini geometrik progressiya bilan oshirmoqda. Professorlar tili bilan aytganda, bu — axborot xavfsizligining "immun tanqisligi" bo‘lib, unda bitta ochiq qolgan texnik tirqish (vulnerability) butun boshli korporativ organizmning o'limiga sabab bo'lishi mumkin.

Raqamli asrda "zaharga qarshi zahar" sifatida faqat doimiy zahira nusxalarini (backup) yaratish va tizimlarni muntazam yangilab borishgina bizni bu kabi algoritmik asirlikdan qutqarib qolishi mumkin.

Kriptojeking (Cryptojacking)

Agar kiberjinoyat olamida "vampirizm" tushunchasi mavjud bo‘lsa, u shubhasiz **kriptojeking** (Cryptojacking) deb ataladi. Bu jinoyat turi boshqa kiber-hujumlardan o‘zining o‘ta yashirinligi va "yumshoq" zarari bilan ajralib turadi. Talaba yoshlar orasida keng tarqalgan "bepul pishloq" — ya’ni turli pullik o‘yinlar yoki professional dasturlarning "crack" (buzilgan) versiyalarini yuklab olish ishtiyoqi ko‘pincha ushbu tuzoqqa kirish eshigi bo‘lib xizmat qiladi.

Ilmiy jihatdan tushuntirganda, kriptojeking — bu foydalanuvchining hisoblash quvvatidan (CPU va GPU resurslaridan) ruxsatsiz foydalangan holda kriptovalyuta (ko‘pincha Monero kabi anonim koinlar) qazib olish (**mining**) jarayonidir. Jinoyatchilar zararli kodni nafaqat yuklab olinadigan fayllar ichiga, balki shubhali veb-saytlarning skriptlariga ham joylashtirishi mumkin. Siz shunchaki biror saytda kino ko‘rayotganingizda, brauzeringiz orqa fonda murakkab matematik amallarni bajara boshlaydi va bu jarayondan tushadigan daromad butunlay jinoyatchining hamyoniga yo‘naltiriladi.

Bu jarayonning foydalanuvchi uchun salbiy oqibatlari bir qarashda sezilmasligi mumkin, ammo vaqt o‘tishi bilan qurilmada "texnik charchoq" alomatlari paydo bo‘ladi: **Termik zo‘riqish:** Protsessorning 100% quvvatda ishlashi natijasida qurilma haddan tashqari qiziydi,

[2] Europol. *WannaCry Ransomware Attack: Lessons Learned*. (2017). Ushbu hisobotda kiber-tahdidlarning global iqtisodiyot va sog‘liqni saqlash tizimlariga ko‘rsatadigan kritik ta’siri statistik ma’lumotlar bilan tahlil qilingan.

bu esa apparat qismlarining (mikrosxemalar, akkumulyator) xizmat muddatini keskin qisqartiradi.

Ish unumdorligining pasayishi: Kompyuter yoki smartfon kutilmaganda "qotib" qolishi, oddiy vazifalarni bajarishda ham sekinlashishi kuzatiladi.

Energiya iste’moli: Qurilma quvvati odatdagidan ancha tez tugaydi va elektr energiyasi sarfi ortadi.

Umuman olganda, kriptojeking — bu foydalanuvchining shaxsiy mulkidan (qurilmasidan) uning xabarisiz iqtisodiy foyda olishga qaratilgan **raqamli parazitizm**dir. Bu turdagi hujumlar kiberxavfsizlikda "ko‘rinmas front" hisoblanadi, chunki u sizning fayllaringizni o‘g‘irlamaydi yoki tizimni bloklamaydi, shunchaki qurilmangizning "hayotiy quvvatini" so‘rib oladi. Shu sababli ham, litsenziyalanmagan dasturlardan foydalanish nafaqat mualliflik huquqining buzilishi, balki o‘z shaxsiy qurilmangizni begona kimsalarning "kripto-fermasi"ga aylantirib qo‘yish xavfini tug‘diradi.

O‘zbekistondagi vaziyat va huquqiy tahlil

O‘zbekiston Respublikasining 2022-yilda qabul qilingan "Kiberxavfsizlik to‘g‘risida"gi qonuni bu sohadagi katta qadam bo‘ldi. Qonunga ko‘ra, kiberxavfsizlikni ta’minlash milliy xavfsizlikning ajralmas qismi deb belgilandi[3].

Shuningdek, JKning 168-moddasi (Firibgarlik) va 169-moddasi (O‘g‘rilik)ga axborot texnologiyalaridan foydalanib sodir etilgan jinoyatlar uchun og‘irroq jazo choralari kiritildi.

Biroq, muammo shundaki, kiberjinoyatlar chegara bilmaydi. Jinoyatchi Afrikada yoki Sharqiy Evropada o‘tirib, O‘zbekistondagi fuqaroni tunashi mumkin. Bunday holatlarda jinoyatchini topish va jazolash xalqaro hamkorlikni talab qiladi, bu esa har doim ham oson kechmaydi.

Xulosa (Conclusion)

Ushbu tadqiqotimizning yakuniy nuqtasi sifatida shuni alohida ta’kidlash lozimki, kiberjinoyatchilik — bu shunchaki dasturiy kodlar o‘rtasidagi "sovuq urush" emas, balki insoniyat sivilizatsiyasining raqamli bosqichidagi o‘ziga xos ekzistensial sinovidir. Tahlillarimiz shuni ko‘rsatdiki, texnologik taraqqiyot qanchalik baland cho‘qqilarga ko‘tarilmasin, kiberxavfsizlik zanjirining eng nozik va ayni paytda eng muhim bo‘g‘ini hamon **inson omili** bo‘lib qolmoqda. Dunyodagi eng mukammal algoritmlar va eng mustahkam mudofaa devorlari ham insonning oddiygina ishonuvchanligi yoki e’tiborsizligi oldida o‘z kuchini yo‘qotishi mumkin. Bu esa kiberxavfsizlikni texnik masaladan ko‘ra ko‘proq psixologik va madaniy fenomen darajasiga ko‘taradi.

Bugungi kunda biz guvohi bo‘layotgan "texnologik qurollanish poygasi", ayniqsa, sun’iy intellektning kiberhujumlarga integratsiyalashuvi, mudofaa strategiyalarimizni tubdan qayta ko‘rib chiqishni taqozo etmoqda. Endilikda biz nafaqat reaktiv (sodir bo‘lgan hodisaga javob beruvchi), balki proaktiv (oldindan ko‘ra biluvchi) tizimlarni yaratishga majburmiz. Bu jarayonda ta’lim tizimining roli beqiyosdir. Kiberxavfsizlik asoslarini o‘qitish shunchaki fakultativ mashg‘ulot emas, balki zamonaviy talaba uchun "raqamli omon qolish san’ati" sifatida ko‘rilishi shart. Zero, raqamli savodxonlik yetishmasligi oqibatida yoshlarning bilib-

[3] O‘zbekiston Respublikasining 2022-yil 15-apreldagi "Kiberxavfsizlik to‘g‘risida"gi O‘RQ-764-son Qonuni, 4-modda. Ushbu qonun bilan kiberfazoda shaxs, jamiyat va davlat manfaatlarini himoya qilishning huquqiy asosi mustahkamlandi.

bilmay kiberjinoyat vositasiga — "kiber-mul"larga aylanib qolishi jamiyat uchun nafaqat iqtisodiy, balki ma’naviy yo‘qotishdir.

Xulosa o‘rnida aytish mumkinki, raqamli dunyoda xavfsizlik — bu erishiladigan yakuniy manzil emas, balki to‘xtovsiz davom etadigan intellektual safardir. Biz "raqamli gigiena"ni shunchaki tavsiyalar ro‘yxati sifatida emas, balki zamonaviy insonning kundalik turmush tarzi va madaniyatining ajralmas qismi sifatida qabul qilishimiz lozim. Murakkab parollar, ikki bosqichli autentifikatsiya va sog‘lom shubha — bular shunchaki texnik cheklovlar emas, balki bizning raqamli erkinligimizni himoya qiluvchi qalqonlardir. Unutmasligimiz kerakki, virtual dunyoda ogohlikni yo‘qotish — real dunyodagi xavfsizlikdan voz kechish bilan barobardir

Foydalanilgan adabiyotlar ro‘yxati:

1. O‘zbekiston Respublikasining "Kiberxavfsizlik to‘g‘risida"gi O‘RQ-764-son Qonuni. (2022).
2. O‘zbekiston Respublikasi Jinoyat Kodeksi.
3. X.M. Muhitsitdinov, "Axborot xavfsizligi va kiberjinoyatchilikka qarshi kurash asoslari". Toshkent: Fan va texnologiya, 2021.
4. Interpol. (2023). *Global Cybercrime Strategy Report.
5. Kaspersky Lab. (2024). *The State of Industrial Cybersecurity in the Era of Digitalization.
6. Usmonov, S. "Ijtimoiy muhandislik: Turlari va himoyalanish usullari". Journal of Digital Law*, 2023