INTERNET JINOYATCHILIGI (KIBERJINOYATLAR): ZAMONAVIY TAHDIDLAR VA ULARNI TARTIBGA SOLISHDAGI HUQUQIY MUAMMOLAR

Bo'riyev Odil Qobilovich
TerDu yuridik fakulteti katta o'qituvchisi
Davronov Bahodir Yahyoyevich
Termiz Davlat universiteti
Yuridik fakulteti, Yurisprudensiya yo'nalishi talabasi

https://doi.org/10.5281/zenodo.19913446

Annotatsiya: *Ushbu maqola zamonaviy axborot texnologiyalari rivojlanishi sharoitida kiberjinoyatchilikning transformatsiyasi, uning turlari va jamiyat xavfsizligiga ta'sirini tahlil qiladi. Tadqiqotda kiberjinoyatlarni xalqaro va milliy darajada huquqiy tartibga solishdagi tizimli muammolar, yurisdiksiya masalalari va qonunchilikdagi bo'shliqlar ilmiy jihatdan asoslab berilgan.*

Kalit so'zlar: *Kiberjinoyat, axborot xavfsizligi, kiberfazo, yurisdiksiya, raqamli dalillar, xalqaro huquq, kiberterrorizm.*

Abstract: *This article analyzes the transformation of cybercrime in the context of modern information technology development, its types, and its impact on social security. The research scientifically substantiates systemic problems in the legal regulation of cybercrimes at international and national levels, jurisdictional issues, and legislative gaps.*

Keywords: *Cybercrime, information security, cyberspace, jurisdiction, digital evidence, international law, cyberterrorism.*

Аннотация: *В данной статье анализируется трансформация киберпреступности в условиях развития современных информационных технологий, её виды и влияние на общественную безопасность. В исследовании научно обоснованы системные проблемы правового регулирования киберпреступлений на международном и национальном уровнях, вопросы юрисдикции и пробелы в законодательстве.*

Ключевые слова: *Киберпреступность, информационная безопасность, киберпространство, юрисдикция, цифровые доказательства, международное право, кибертерроризм.*

Kirish: Global raqamlashtirish jarayoni insoniyat sivilizatsiyasini yangi bosqichga olib chiqish bilan birga, ijtimoiy xavfli qilmishlarning yangi shakli — kiberjinoyatchilik fenomenini yuzaga keltirdi. Bugungi kunda kiberjinoyatlar nafaqat iqtisodiy zarar yetkazuvchi, balki davlatning suvereniteti va milliy xavfsizligiga tahdid soluvchi global muammoga aylandi. Kiberfazo chegarasiz xarakterga ega ekanligi, jinoyatchilarga anonimlik va masofadan turib harakat qilish imkoniyatini berishi huquqni muhofaza qiluvchi organlar oldida murakkab vazifalarni qo'ymoqda. Insoniyatning raqamli makonga migratsiyasi "virtual reallik" tushunchasini kundalik hayotning ajralmas qismiga aylantirdi. Biroq, bu progress "kiber-deviatsiya" deb ataluvchi salbiy ijtimoiy hodisaning kengayishiga zamin yaratdi.

Kiberjinoyatchilik an'anaviy jinoyatchilikdan o'zining transchegaraviyligi, anonimligi va yuqori latentliligi (yashirinligi) bilan farq qiladi. Ilmiy nuqtai nazardan, kiberfazo jinoyatchi uchun "chegarasiz poligon" vazifasini o'tamoqda, bu yerda davlat suvereniteti tushunchasi klassik geografik chegaralar bilan cheklanib qolmaydi. Hozirgi kunda kiberjinoyatlarning iqtisodiy zarari jahon yalpi ichki mahsulotining (YIM) sezilarli qismini tashkil etmoqda, bu esa ushbu muammoni nafaqat huquqiy, balki makroiqtisodiy xavfsizlik darajasiga ko'taradi.

Asosiy qismi: 1. Zamonaviy kiber-tahdidlarning tipologik tahlili

Hozirgi vaqtda kiberjinoyatchilikning dinamikasi uning texnik murakkabligini oshirib bormoqda. Asosiy tahdidlar sirasiga quyidagilarni kiritish mumkin:

Kiber-josuslik va davlat darajasidagi hujumlar: Muhim infratuzilmalarni (energetika, moliya, mudofaa) ishdan chiqarishga qaratilgan maqsadli hujumlar (Threats from Cyberspace).

Ransomware (Tovlamachi dasturlar): Ma'lumotlarni shifrlash orqali yirik korporatsiyalar va davlat organlaridan kriptovalyuta shaklida haq talab qilish.

Ijtimoiy muhandislik va fishing: Inson omilidan foydalangan holda maxfiy ma'lumotlarni o'g'irlash.

2. Huquqiy tartibga solishdagi tizimli muammolar

Kiberjinoyatchilikka qarshi kurashda huquqiy doktrina bir qator fundamental to'siqlarga duch kelmoqda:

Yurisdiksiya muammosi: Jinoyat obyekti bir davlatda, subyekti ikkinchi davlatda, oqibati esa uchinchi davlatda yuzaga kelishi qaysi davlat qonunchiligini qo'llash masalasini murakkablashtiradi.

Raqamli dalillarning protsessual maqomi: Elektron ma'lumotlarning tez o'zgaruvchanligi va yo'qolib ketish ehtimoli yuqoriligi sababli, ularni protsessual qat'iy mustahkamlash mexanizmlari hali mukammal emas.

Xalqaro hamkorlikning sustligi: Budapesht konvensiyasi (2001) kabi hujjatlar mavjudligiga qaramay, barcha davlatlar kiberfazo ustidan nazorat o'rnatishda yagona konsensusga ega emas.(Zaitov, A 2021 Kiberjinoyatchilikning kriminologik tavsifi.Toshkent: TDYU)

3. Normativ-huquqiy bazani takomillashtirish zaruriyati

O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni va Jinoyat kodeksidagi tegishli o'zgartirishlar muhim qadam bo'ldi. Biroq, sun'iy intellekt (AI) yordamida sodir etiladigan jinoyatlarning (Deepfake, avtonom kiberhujumlar) huquqiy kvalifikatsiyasi hali ham ochiq qolmoqda. .(O'zbekiston Respuplikasi "Kiberxavfsizlik to'g'risida"gi Qonun 2022)

4. Kiberjinoyatchilikning kriminologik determinatsiyasi

Kiberjinoyatchilikning o'sishiga sabab bo'layotgan omillarni bir necha guruhga ajratish mumkin:

Texnologik omillar: Dasturiy ta'minotlardagi zaifliklar (vulnerabilities) va kiberhujum vositalarining (masalan, "DarkNet"dagi tayyor exploitlar) ommaviylashuvi.

Ijtimoiy-iqtisodiy omillar: Yuqori daromad olish imkoniyati va jinoyat sodir etish xarajatlarining nisbatan pastligi.

Huquqiy nigilizm: Foydalanuvchilarning kiber-gigiyena qoidalariga rioya qilmasligi va raqamli makonda jazo muqarrarligi mexanizmining sustligi.

5. Kiber-sub'ektlar va ularning tasnifi

Ilmiy adabiyotlarda kiberjinoyatchilar motivatsiyasiga ko'ra quyidagicha klassifikatsiya qilinadi:

Xaker-idealistlar (Hacktivists): Siyosiy yoki ijtimoiy g'oyalar yo'lida hujum uyushtiruvchilar.

Kiber-terrorchilar: Davlat xavfsizligiga tahdid solish va aholi orasida vahima uyg'otishni maqsad qilgan guruhlar.

Davlat tomonidan qo'llab-quvvatlanadigan guruhlar (State-sponsored actors): Boshqa davlatlarning iqtisodiy va harbiy sirlarini o'g'irlashga ixtisoslashgan sub'ektlar.

6. Raqamli dalillarni to'plashdagi kollizion normalar

Kiberjinoyatlarni tergov qilishda eng katta to'siq — elektron dalillarning beqarorligi (volatile nature). Ma'lumotlar soniyalar ichida masofadan turib o'chirib yuborilishi yoki o'zgartirilishi mumkin.

Bulutli hisoblashlar (Cloud Computing): Ma'lumotlar serveri boshqa davlatda joylashgan bo'lsa, uni huquqiy yo'l bilan olish oylab vaqt talab qiladi, bu esa "tezkor tergov" tamoyiliga zid keladi.

Kriptografik to'siqlar: Shifrlangan ma'lumotlarni dekodlashda inson huquqlari (shaxsiy hayot daxlsizligi) va tergov manfaatlari o'rtasidagi muvozanatni saqlash masalasi dolzarbligicha qolmoqda.

7. Kiberxavfsizlikda Sun'iy Intellekt (AI) roli: "Ikki tomonlama tig'"

Sun'iy intellekt texnologiyalari kiberjinoyatchilikda yangi davrni boshlab berdi. Bir tomondan, AI yordamida kiberhujumlarni avtomatlashtirish va "Deepfake" texnologiyasi orqali yirik firibgarliklarni amalga oshirish xavfi ortgan bo'lsa, ikkinchi tomondan, AI tahdidlarni erta aniqlash va ularga javob qaytarishda asosiy vosita bo'lib xizmat qilmoqda.

8. Kiberjinoyatlarning transchegaraviy tabiati va milliy suverenitet to‘qnashuvi

Kiberjinoyatchilik an’anaviy huquqiy tushuncha bo‘lmish "hududiy suverenitet" prinsipiga jiddiy sinov hisoblanadi. Ilmiy nuqtai nazardan, kiberfazo davlatlararo chegaralarni virtual darajada yo‘q qilib yuborgan.

Eksterritoriallik muammosi: Jinoyatchi bir mamlakatda turib, boshqa bir mamlakatdagi serverlar orqali uchinchi mamlakat fuqarolariga zarar yetkazishi mumkin. Bunda qaysi davlatning jinoyat qonunchiligi ustuvor bo‘lishi (Lex loci delicti) haqida huquqiy kolliziya yuzaga keladi.

Ma’lumotlar lokalizatsiyasi: Ko‘pgina davlatlar o‘z fuqarolarining shaxsiy ma’lumotlarini mamlakat hududidagi serverlarda saqlash talabini (Data Residency) qo‘ymoqda. Bu kiberxavfsizlikni oshirsa-da, xalqaro tergov jarayonida ma’lumot almashinuvini byurokratik jihatdan qiyinlashtiradi.

9. Raqamli kriminologiya: Viktimologik tahlil

Kiberjinoyatlarning o‘sishi nafaqat texnik zaifliklar, balki foydalanuvchilarning viktimallik (jabrlanuvchi bo‘lishga moyillik) darajasi bilan ham bog‘liq.

Raqamli savodxonlik yetishmasligi: Ko‘p hollarda kiberhujumlar murakkab kodlar orqali emas, balki oddiy insoniy xatolar — "ijtimoiy muhandislik" (social engineering) orqali amalga oshiriladi.

Anonimlik va psixologik inhibitivlik: Kiberfazoda jinoyatchi jabrlanuvchini ko‘rmaydi, bu esa unda jinoyat uchun axloqiy mas’uliyat hissini kamaytiradi va qilmishning og‘irlik darajasini sub’ektiv idrok etishga to‘sqinlik qiladi.

10. Kiberjinoyatchilikka qarshi kurashda davlat-xususiy sheriklik (PPP) modeli

Ilmiy tadqiqotlar shuni ko‘rsatadiki, davlat kiberjinoyatchilikka qarshi yakka tartibda kurasha olmaydi. Chunki:

Infratuzilmaning xususiy qo‘llarda ekanligi: Internet-provayderlar, bank tizimlari va bulutli xizmatlarning katta qismi xususiy sektorga tegishli.

Texnologik ustunlik: IT-kompaniyalar yangi turdagi tahdidlarni davlat organlaridan ko‘ra tezroq aniqlash imkoniyatiga ega.

Shu sababli, huquqiy tartibga solishda xususiy sektorga "operativ axborot almashish" va "kiber-gigiyenani ta’minlash" bo‘yicha qo‘shimcha huquqiy majburiyatlar yuklash yoki

rag‘batlantirish mexanizmlarini yaratish lozim.

11. Kriptovalyutalar va jinoiy daromadlarni legallashtirish

Kiberjinoyatchilikning moliya tizimi bugungi kunda an’anaviy banklardan blokcheyn texnologiyasiga o‘tgan.

Kripto-aktivlarning anonimligi: Jinoyat yo‘li bilan topilgan mablag‘larni "mikserlar" va "tunnellar" orqali yuvish, huquqni muhofaza qiluvchi organlar uchun mablag‘lar oqimini kuzatishni imkonsiz darajaga keltiradi.

Huquqiy bo‘shliq: Ko‘plab mamlakatlarda kripto-aktivlarning huquqiy maqomi hali ham aniq belgilanmagan, bu esa jinoiy daromadlarni musodara qilishda protsessual muammolarni keltirib chiqarmoqda.

12. Kiber-makonda "Jinoyat quroli" tushunchasining transformatsiyasi

An'anaviy huquqda jinoyat quroli moddiy xususiyatga ega bo'lsa, kiberjinoyatlarda bu tushuncha virtual shaklga o'tadi.

Dasturiy kod — qurol sifatida: Zararli dasturlar (malware), viruslar va troyanlar nafaqat ma'lumot o'g'irlash, balki real dunyodagi ob'ektlarga (masalan, atom elektrostansiyalari yoki suv tozalash inshootlari) zarar yetkazish quroliga aylandi.

Botnetlar va ularning huquqiy kvalifikatsiyasi: Minglab "zombi-kompyuterlar"dan tashkil topgan tarmoqlar orqali amalga oshiriladigan DDoS hujumlari kollektiv jinoyatchilikning yangi shakli sifatida qaralishi lozim. Bu yerda kompyuter egasining (bilmagan holda) jinoyatdagi ishtiroki masalasi murakkab huquqiy muammo hisoblanadi.(Rustambayev, M.H. 2020 O’zbekiston Respublikasi Jinoyat huquqi kursi. Toshkent.)

13. Kiber-protsessual huquqda "Dalillar zanjiri" (Chain of Custody)

Raqamli dalillar bilan ishlashda ularning haqiqiyligini saqlab qolish eng ustuvor vazifa hisoblanadi.

Hesh-funksiyalar roli: Raqamli dalil olingan vaqtda uning "raqamli barmoq izi" (hash) hisoblanishi va sud jarayonigacha u o'zgarmaganligini isbotlash mexanizmi qat'iy tartibga solinishi kerak.

Adliya texnologiyalari (Digital Forensics): Ma'lumotlarni o'chirilgandan so'ng ham tiklash imkonini beruvchi texnologiyalar sud-ekspertiza amaliyotida alohida yo'nalish sifatida huquqiy maqomga ega bo'lishi shart.

14. "Deepfake" va dezinformatsiya: Shaxs daxlsizligiga yangi tahdidlar

Sun'iy intellekt yordamida inson tasviri va ovozini o'zgartirish (Deepfake) kiberjinoyatchilikning eng xavfli turlaridan biriga aylandi.

Siyosiy va ijtimoiy manipulyatsiya: Soxta videolar orqali jamiyatda tartibsizliklar keltirib chiqarish kiber-terrorizmning tarkibiy qismi sifatida baholanishi mumkin.

Huquqiy himoya yetishmovchiligi: O'zbekiston va ko'plab xorijiy davlatlar qonunchiligida "deepfake" orqali yetkazilgan ma'naviy va moddiy zararni qoplash bo'yicha aniq normalar shakllanib ulgurmagan.

15. Kiber-gigiyena va huquqiy tarbiya: Davlat siyosatining ustuvor yo'nalishi

Kiberjinoyatchilikka qarshi kurash faqat jazo choralari bilan cheklanib qolmasligi kerak.

Preventiv choralar: "Kiber-savodxonlik" tushunchasini ta'lim tizimiga kiritish va aholining raqamli madaniyatini yuksaltirish orqali kiber-viktimallikni (jabrlanuvchi bo'lish xavfini) kamaytirish.

Etik xakerlik (White Hat Hacking): Davlat tizimlaridagi zaifliklarni aniqlash uchun ijobiy maqsadli xakerlarni jalb qilishning huquqiy mexanizmlarini yaratish.

TAVSIYALAR:

Ushbu muammolarni bartaraf etish uchun quyidagi ilmiy-amaliy takliflar ilgari suriladi:

"Raqamli kriminallashuv" tushunchasini kengaytirish: Jinoyat kodekslariga nafaqat kompyuter tizimiga hujum, balki raqamli manipulyatsiya va AI vositasida sodir etilgan intellektual firibgarliklarni ham qat'iy kiritish.

Tezkor elektron o'zaro hamkorlik tizimi: Davlatlararo darajada sud qarorisiz, faqat tergov organi so'rovi bilan "elektron izlarni" zudlik bilan muzlatish (preservation) mexanizmini joriy etish.

Kiber-prokuratura va kiber-sud tizimini shakllantirish: Sudyalarning raqamli dalillar va axborot texnologiyalari bo'yicha ixtisoslashgan malakasini oshirish.

Xulosa: Ilmiy tahlillar shuni ko'rsatadiki, kiberjinoyatchilikka qarshi samarali kurashish uchun quyidagi chora-tadbirlarni amalga oshirish zarur:

Universal xalqaro konvensiyani qabul qilish: BMT shafeligida barcha davlatlar uchun majburiy bo'lgan yagona huquqiy normativ hujjat ishlab chiqish.

Raqamli kriminologiyani rivojlantirish: Kiberjinoyatchilarning psixologik portreti va yangi usullarini bashorat qiluvchi ilmiy markazlarni tashkil etish.

Yurisdiktsiyani kengaytirish: "Kiber-suverenitet" va "eksterritorial yurisdiksiya" tushunchalarini milliy qonunchilikda aniq belgilash.

Foydalanilgan adabiyotlar:

1. Brenner, S. W. (2012). Cybercrime: Criminal Threats from Cyberspace. ABC-CLIO.
2. Clough, J. (2015). Principles of Cybercrime. Cambridge University Press.
3. Kshetri, N. (2010). The Global Cybercrime Industry. Springer Science & Business Media.
4. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni, 2022.
5. Zaitov, A. (2021). Kiberjinoyatchilikning kriminologik tavsifi. Toshkent: TDYU.
6. Gercke, M. (2012). Understanding Cybercrime: Phenomena, Challenges and Legal Response. ITU.
7. Grabosky, P. (2016). Cybercrime. Oxford University Press.
8. Wall, D. S. (2007). Cybercrime: The Transformation of Crime in the Information Age. Polity Press.
9. Yar, M., & Steinmetz, K. F. (2019). Cybercrime and Society. SAGE Publications.
10. United Nations Office on Drugs and Crime (UNODC). (2013). Comprehensive Study on Cybercrime.
11. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention).
12. Rustambayev, M.H. (2020). O'zbekiston Respublikasi Jinoyat huquqi kursi. Toshkent.
13. Lessig, L. (2006). Code: And Other Laws of Cyberspace. Basic Books.
14. Broadhurst, R. (2006). "Developments in the global law enforcement of cyber-crime". Policing: An International Journal.
15. Karimov, A.A. (2023). "Axborot texnologiyalari sohasidagi jinoyatlarni tergov qilish metodikasi". Huquqiy tadqiqotlar jurnali.