KIBERJINOYATCHILIK VA RAQAMLI XAVFSIZLIK: RAQAMLI ASRDA QONUN VA JAVOBGARLIK

Gulomov Abdulaxadxon Baxtiyor o'g'li
Namangan davlat universiteti
Yuridik fakulteti 2-bosqich talabasi
Email: abdulahadgulomov5050@icloud.com
https://orcid.org/0009-0004-6668-692X
https://doi.org/10.5281/zenodo.21927538

Annotatsiya: Ushbu ilmiy-amaliy va huquqiy tadqiqot ishida axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi sharoitida kiberjinoyatchilikning rivojlanish dinamikasi, uning zamonaviy ko'rinishlari hamda raqamli xavfsizlikni ta'minlashning huquqiy va tashkiliy-texnik mexanizmlari atroflicha tahlil qilinadi. Tadqiqotda kiberjinoyatlarning tasnifi, transchegaraviy xususiyati, kripto-aktivlar va sun'iy intellekt texnologiyalaridan noqonuniy foydalanish holatlari yoritilgan. Shuningdek, O'zbekiston Respublikasining kiberxavfsizlik sohasidagi milliy qonunchilik bazasi (xususan, "Kiberxavfsizlik to'g'risida"gi va "Shaxsga doir ma'lumotlar to'g'risida"gi qonunlar) va xalqaro huquqiy normalar (Budapesht konvensiyasi, BMT tashabbuslari) qiyosiy-huquqiy jihatdan o'rganilgan. Maqolada raqamli dalillarni to'plash (digital forensics), yurisdiksiya toqnashuvlari hamda raqamli makonda javobgarlikni belgilash muammolari ko'rib chiqilib, milliy qonunchilik va huquqni muhofaza qilish amaliyotini takomillashtirish bo'yicha ilmiy-amaliy takliflar ilgari surilgan.

Kalit so'zlar: kiberjinoyatchilik, raqamli xavfsizlik, kiberxavfsizlik, raqamli dalillar, yurisdiksiya, Budapesht konvensiyasi, kibertahdidlar, axborot daxlsizligi, kiberforinzika, jinoiy javobgarlik.

CYBERCRIME AND DIGITAL SECURITY: LAW AND LIABILITY IN THE DIGITAL AGE

Gulomov Abdulakhadkhon
2nd year student of the Faculty of Law of NamSU

Abstract: This comprehensive research paper explores the dynamics of cybercrime, its modern manifestations, and the legal and organizational-technical mechanisms for ensuring digital security in the era of rapid information and communication technology advancement. The study analyzes the classification of cybercrimes, their transboundary nature, and the illicit use of crypto-assets and artificial intelligence technologies. A comparative legal analysis is conducted between Uzbekistan's national legislative framework on cybersecurity (specifically the Laws "On Cybersecurity" and "On Personal Data") and international standards (including the Budapest Convention and UN initiatives). The article highlights critical challenges surrounding digital evidence collection (digital forensics), jurisdictional conflicts, and the attribution of criminal liability in cyberspace. Finally, it provides practical and scientific recommendations aimed at improving national legislation and law enforcement practices.

Keywords: cybercrime, digital security, cybersecurity, digital evidence, jurisdiction, Budapest Convention, cyber threats, data privacy, digital forensics, criminal liability.

КИБЕРПРЕСТУПНОСТЬ И ЦИФРОВАЯ БЕЗОПАСНОСТЬ: ЗАКОН И ОТВЕТСТВЕННОСТЬ В ЦИФРОВУЮ ЭРУ

Гуломов Абдулахадхон
Студентка 2 курса юридического факультета НамГУ

Аннотация: В данном комплексном научном исследовании подробно анализируются динамика развития киберпреступности, её современные формы, а также правовые и организационно-технические механизмы обеспечения цифровой безопасности в условиях стремительного прогресса информационно-коммуникационных технологий. В работе рассмотрены классификация киберпреступлений, их трансграничный характер, а также случаи неправомерного использования криптоактивов и технологий искусственного интеллекта. Проведен сравнительно-правовой анализ национального законодательства Республики Узбекистан в сфере кибербезопасности (в частности, законов «О кибербезопасности» и «О персональных данных») и международных правовых норм (Будапештская конвенция, инициативы ООН). Рассматриваются проблемы сбора цифровых доказательств (digital forensics), юрисдикционных конфликтов и установления ответственности в цифровом пространстве, а также приводятся научно-практические рекомендации по совершенствованию законодательства и правоприменительной практики.

Ключевые слова: киберпреступность, цифровая безопасность, кибербезопасность, цифровые доказательства, юрисдикция, Будапештская конвенция, киберугрозы, конфиденциальность информации, киберфорензика, уголовная ответственность.

Aholi hayotining barcha jabhalariga raqamli texnologiyalar, sun’iy intellekt, buyumlarning interneti (IoT) va bulutli hisoblash tizimlarining jadal kirib kelishi insoniyat tamaddunida to‘rtinchi sanoat inkilobini boshlab berdi. Iqtisodiyot, davlat boshqaruvi, moliya-bank sektori va ijtimoiy munosabatlarning raqamlashtirilishi bir tomondan samaradorlik va qulaylikni oshirgan bo‘lsa, ikkinchi tomondan insoniyatni yangi turdagi global tahdid — kiberjinoyatchilik bilan yuzma-yuz qoldirdi. Bugungi kunda kiberjinoyatchilik shunchaki yakka tartibdagi hakerlarning texnik bezoriligi darajasidan chiqib, xalqaro darajada uyushgan, ko‘p milliardli daromad keltiruvchi va davlatlarning milliy xavfsizligiga bevosita tahdid soluvchi xalqaro jinoiy industriyaga aylandi. Kiberhujumlar natijasida muhim axborot infratuzilmalari (elektr tarmoqlari, sog‘liqni saqlash tizimlari, bank tarmoqlari) ishdan chiqishi, maxfiy davlat va tijorat ma’lumotlari hamda millionlab fuqarolarning shaxsga doir ma’lumotlari sizdirilishi kuzatilmoqda. Ushbu sharoitda an’anaviy huquq tizimlari va huquqni muhofaza qiluvchi organlar jiddiy muammolar bilan to‘qnash kelmoqda. Virtual makonning chegarasizligi (transchegaraviyligi), anonimlikni ta’minlovchi texnologiyalarning (VPN, TOR, mikser-servislar, kriptovalyutalar) mavjudligi hamda raqamli izlarning tez o‘chib ketishi kiberjinoyatlarni tergov qilish va aybdorlarni javobgarlikka tortishni murakkablashtiradi.

Ushbu tadqiqotning maqsadi kiberjinoyatchilikning zamonaviy tendensiyalarini, raqamli xavfsizlikni ta’minlashning nazariy va amaliy jihatlarini o‘rganish, O‘zbekiston Respublikasi va xalqaro tajriba misolida raqamli makonda qonuniylik va javobgarlikni ta’minlash mexanizmlarini takomillashtirish bo‘yicha ilmiy xulosalar ishlab chiqishdan iborat.

I BOB. KIBERJINOYATCHILIKNING NAZARIY VA HUQUQIY ASOSLARI

1.1. "Kiberjinoyatchilik" va "Raqamli Xavfsizlik" tushunchalarining mohiyati: Huquqshunoslik va axborot texnologiyalari fanida "kiberjinoyatchilik" (cybercrime) va "raqamli xavfsizlik" (digital security / cybersecurity) tushunchalariga turlicha ta’riflar beriladi.

- Kiberjinoyatchilik — kompyuter texnikasi, axborot tizimlari va telekommunikatsiya tarmoqlaridan foydalangan holda yoki ularga bevosita hujum qilish orqali sodir etiladigan, jamiyat, davlat, yuridik va jismoniy shaxslarning qonun bilan qo‘riqlanadigan manfaatlariga zarar yetkazuvchi g‘ayriqonuniy qilmishlar majmuidir.
- Raqamli xavfsizlik (Kiberxavfsizlik) — bu kibermakonda shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holati bo‘lib, u axborotning konfidentsialligi (maxfiyligi), yaxlitligi(o‘zgarmasligi) va foydalanish imkoniyati (yo‘l qo‘yilganligi) kabi uchta asosiy ustunga (CIA triad) tayanadi.

Kiberjinoyat sifatidagi qilmishlarni shartli ravishda ikki guruhga ajratish mumkin:

1. Kompyuterga yo‘naltirilgan jinoyatlar (Cyber-dependent crimes): Axborot tizimlari va tarmoqlarisiz sodir etilishi mumkin bo‘lmagan jinoyatlar (masalan, zararli dasturlarni (malware) tarqatish, DDoS hujumlari, axborot tizimini buzib kirish).
2. Kompyuter vositachiligidagi jinoyatlar (Cyber-enabled crimes): An’anaviy jinoyatlarning raqamli vositalar yordamida sodir etilishi (masalan, internet orqali firibgarlik, raqamli tovlamachilik, noqonuniy savdo, shaxsiy hayot daxlsizligini buzish).

1.2. Kiberjinoyatchilikning rivojlanish tarixi va zamonaviy tendensiyalari: Kiberjinoyatchilik rivojlanishi uch asosiy bosqichni bosib o‘tdi:

[1-bosqich: 1970-1990-yillar] ⟶ Individual hakerlik va bilim namoyishi (Phone phreaking, birinchi kompyuter viruslari - Morris qurtlari).

[2-bosqich: 2000-2010-yillar] ⟶ Tijoratlashtirish va moliyaviy manfaat (Spam, bank troyanlari, shaxsiy ma'lumotlarni o'g'irlash).

[3-bosqich: 2010-yildan hozirgacha] ⟶ Professional jinoiy sindikatlar, kiberurushlar, AI va Ransomware-as-a-Service (RaaS).

Bugungi kunda kiberjinoyatchilikning asosiy tendensiyalari quyidagilardan iborat:

- Sanoatlashuv va Ransomware-as-a-Service (RaaS): Tovlamachi dasturlarni yaratuvchilar ularni franshiza sifatida boshqa kichik jinoiy guruhlarga taqdim etadi.
- Sun’iy Intellekt va Deepfake: AI yordamida fishing xabarlarini avtomatlashtirish, inson ovozi hamda tasvirini qalbakilashtirish orqali muassasalar va fuqarolarni chalg‘itish.
- Kriptovalyutalar va Mikserlar: Jinoiy yo‘l bilan topilgan mablag‘larni yuvish uchun blokcheyn texnologiyalari va anonim kripto-aktivlardan foydalanish.

II BOB. KIBERJINOYATLARNING ASOSIY TURLARI VA ULARNING JAMIYATGA TA'SIRI

2.1. Zamonamizning eng xavfli kiber-tahdidlari: Kiberjinoyatchilikning turli-tuman shakllari mavjud bo‘lib, ularning eng keng tarqalgan va moliyaviy hamda ijtimoiy ziyon yetkazuvchi turlari quyidagi jadvalda aks ettirilgan:

Jinoyat turi	Taktik mexanizmi	Asosiy maqsadi / Oqibati
Ransomware (Tovlamachi dasturlar)	Tizim ma’lumotlarini shifrlab qo‘yish va kalit uchun to‘lov (kriptovalyutada) talab qilish	Tashkilotlar faoliyatini falajlash, moliyaviy tovlamachilik
Phishing / Social Engineering	Soxta veb-saytlar, e-mail va xabarlar orqali foydalanuvchi ishonchiga kirish	Maxfiy login/parollar va bank karta ma’lumotlarini o‘g‘irlash
DDoS Hujumlar	Serverlarga sun’iy ravishda millionlab so‘rovlar yuborib, ularni ishdan chiqarish	Onlayn xizmatlar barqarorligini buzish, obro‘sizlantirish
Identity Theft (Shaxsiyatni o‘g‘irlash)	Boshqa shaxsning raqamli ma’lumotlarini qo‘lga kiritib, uning nomidan harakat qilish	Noqonuniy kreditlar olish, firibgarlik sodir etish
Supply Chain Attacks (Ta’minot zanjiri hujumlari)	Dasturiy ta’minot ishlab chiquvchi uchinchi tomon tizimlarini zararlash	Yirik korporatsiyalar va davlat idoralariga ommaviy kirish

2.2. Muhim axborot infratuzilmasiga (MAI) kiberhujumlar

Zamonaviy davlatlarning hayotiy faoliyati, xususan:

- Energetika tizimlari (elektr stansiyalari, gaz quvurlari),
- Transport va logistika boshqaruvi (aeroportlar, temir yo‘llar),
- Moliya va bank sektori,
- Sog‘liqni saqlash muassasalari

raqamli boshqaruv platformalariga (SCADA, ICS) bog‘liq. Ushbu ob’ektlarga qilingan kiberhujumlar nafaqat axborot yo‘qotilishiga, balki real insonlar hayotiga tahdid soluvchi va texnogen falokatlarga olib keluvchi oqibatlarni keltirib chiqaradi.

III BOB. O‘ZBEKISTON RESPUBLIKASI VA XALQARO QONUNCHILIKDA KIBERXAVFSIZLIKNI TARTIBGA SOLISH

3.1. Milliy huquqiy baza: Yutuqlar va bo‘shliqlar

O‘zbekiston Respublikasida so‘nggi yillarda raqamli xavfsizlikni huquqiy tartibga solish bo‘yicha salmoqli ishlar amalga oshirildi.

1. O‘zbekiston Respublikasining "Kiberxavfsizlik to‘g‘risida"gi Qonuni (2022-yil):
   - Qonun milliy kiberxavfsizlik sub’ektlari, ularning huquq va majburiyatlarini belgilab berdi.
   - Davlat xavfsizlik xizmati (DXX) kiberxavfsizlik sohasidagi vakolatli davlat organi etib belgilandi.

- Muhim axborot infratuzilmasi ob'ektlarining reestri va ularni himoya qilish talablari joriy etildi.

2. O'zbekiston Respublikasi Jinoyat Kodeksi (JK):

- JKning XVI[1] bobi "Axborot texnologiyalari sohasidagi jinoyatlar"ga bag'ishlangan bo'lib, unda kompyuter axborotidan g'ayriqonuniy foydalanish (278[1]-modda), zararli dasturlarni yaratish va tarqatish (278[4]-modda) kabi qilmishlar uchun jinoiy javobgarlik nazarda tutilgan.
- Shuningdek, axborot texnologiyalaridan foydalanib firibgarlik qilish (168-modda) va o'g'rilik sodir etish (169-modda) kabi holatlar og'irlashtiruvchi holat sifatida malakalanadi.

3. "Shaxsga doir ma'lumotlar to'g'risida"gi Qonun (2019-yil):

- Fuqarolarning raqamli muhitdagi shaxsiy daxlsizligini ta'minlash, shaxsga doir ma'lumotlar bazalarini O'zbekiston hududida lokalizatsiya qilish talablarini belgilaydi.

3.2. Xalqaro huquqiy mexanizmlar va transchegaraviy hamkorlik: Kiberjinoyatchilik chegara bilmasligi sababli unga qarshi kurashda xalqaro hamkorlik hal qiluvchi ahamiyatga ega.

- Budapesht Konvensiyasi (2001-yil): Yevropa Kengashining Kiberjinoyatchilik to'g'risidagi konvensiyasi bo'lib, u kiberjinoyatlar bo'yicha milliy qonunlarni uyg'unlashtirish va davlatlaro tezkor hamkorlikni (24/7 tarmoq) yo'lga qo'yishdagi asosiy xalqaro hujjat hisoblanadi.
- BMT doirasidagi tashabbuslar: BMT Hukumatlararo ekspertlar guruhi hamda Ochiq tarkibli ishchi guruhi (OEWG) kibermakonda davlatlarning mas'uliyatli xulq-atvor normalarini ishlab chiqish ustida ish olib bormoqda.
- Interpol va Yevropol: Kiberjinoyatlarni tezkor-qidiruv va xalqaro tergov doirasida muvofiqlashtiruvchi organlar.

IV BOB. RAQAMLI ASDA JAVOBGARLIK VA YURISDIKSIYA MUAMMOLARI

4.1. Transchegaraviylik va Yurisdiksiya toqnashuvi

Kiberjinoyatchilikni tergov qilishda eng katta huquqiy tosiq — bu yurisdiksiya masalasidir. Masalan, O'zbekistondagi bank mijoziga hujum qilgan haker Sharqiy Yevropada joylashgan bo'lishi, buyruqlarni Boshqa qit'adagi server orqali yuborishi, noqonuniy mablag' esa Osiyo mamlakatidagi kripto-birjada naqdlashtirilishi mumkin.

Bu holatda quyidagi muammolar kelib chiqadi:

1. Hududiylik tamoyilining cheklanganligi: Jinoyat sodir etilgan joyni aniq belgilashning murakkabligi.
2. Ekstraditsiya muammosi: Ko'plab davlatlar o'z fuqarolarini chet elga topshirishni taqiqlaydi.
3. Eltib berish muddati: An'anaviy xalqaro huquqiy yordam ko'rsatish so'rovlari (MLAT) oylab va hatto yillab vaqt oladi, raqamli dalillar esa bir necha daqiqada o'chirib tashlanishi mumkin.

4.2. Raqamli dalillar va Kiberforinzika (Digital Forensics)

An'anaviy jinoyatlardan farqli o'laroq, kiberjinoyatlarda dalillar elektron ko'rinishda (server loglari, IP manzillar, shifrlangan fayllar, ram-dump) bo'ladi.

Raqamli dalillarning xususiyatlari:

- O'tkinchilik (Volatility): Elektr manbaidan uzilganda yoki tizim qayta yuklanganda yo'qolishi.

- Oson o‘zgartiriluvchanlik: Professional bilimsiz ko‘zdan kechirish dalilning haqiqiyligiga putur yetkazishi mumkin.

Shu sababli, Jinoyat-protsessual qonunchiligida raqamli dalillarni olib qo‘yish, ko‘zdan kechirish va dalil sifatida maqbul deb topishning maxsus tartiblarini mustahkamlash talab etiladi.

Ushbu tadqiqot natijalariga tayanib, raqamli asrda kiberjinoyatchilikka qarshi samarali kurashish va raqamli xavfsizlikni ta’minlash bo‘yicha quyidagi ilmiy-amaliy tavsiyalar ilgari suriladi:

1.Milliy Qonunchilikni Takomillashtirish va Unifikatsiya Qilish:Huquqiy bazani xalqaro standartlarga moslashtirish.

O‘zbekiston Respublikasi Jinoyat hamda Jinoyat-protsessual kodekslariga kiberjinoyat sifatidagi yangi qilmishlar (masalan, kiber-stalking, ransomware tarqatishning alohida tarkibi, raqamli dalillarni ko‘zdan kechirish tartiblari) bo‘yicha o‘zgartishlar kiritish va O‘zbekistonning Budapesht konvensiyasiga qo‘shilishi maqsadga muvofiqdir.

2.Tezkor Xalqaro Hamkorlik Mexanizmlarini Kuchaytirish:Kiber-politsiya tarmog'ini kengaytirish.

Xalqaro kiberjinoyatlarni tezkor tergov qilish uchun real vaqt rejimida (24/7) ishlaydigan xalqaro kontakt punktlari bilan integratsiyani chuqurlashtirish va kripto-aktivlar harakatini kuzatuvchi maxsus analitik vositalarni amaliyotga joriy etish.

3.Kiberxavfsizlik Sohasida Kadrlar Salohiyatini Oshirish:Kiber-forinzika va tergovchilar tayyorlash.

Huquqni muhofaza qiluvchi organlar xodimlari, sudya va prokurorlar uchun kiber-forinzika, raqamli izlarni to‘plash va tahlil qilish bo‘yicha doimiy malaka oshirish tizimini va ixtisoslashtirilgan kiber-laboratoriyalarni tashkil etish.

4.Aholi va Kichik Biznesning Kiber-gigiyenasini Yuksaltirish:Ijtimoiy muhandislik va phishingga qarshi profilaktika.

Kiberjinoyatlarning aksariyati inson omili (social engineering) orqali sodir etilishini inobatga olib, aholining raqamli savodxonligini oshirish bo‘yicha davlat darajasidagi targ‘ibot va profilaktika dasturlarini muntazam amalga oshirish.

Adabiyotlar, References, Литературы:

1. O‘zbekiston Respublikasining "Kiberxavfsizlik to‘g‘risida"gi Qonuni. – T.: 2022-yil 15-aprel, O‘RQ-764-son.
2. O‘zbekiston Respublikasining "Shaxsga doir ma’lumotlar to‘g‘risida"gi Qonuni. – T.: 2019-yil 2-iyul, O‘RQ-547-son.
3. O‘zbekiston Respublikasining Jinoyat kodeksi (rasmiy matn). – Toshkent: Adolat, 2023.
4. Council of Europe. *Convention on Cybercrime (Budapest Convention)*. ETS No. 185, Budapest, 2001.
5. United Nations General Assembly. *Developments in the field of information and telecommunications in the context of international security*. UN Resolution A/RES/75/240.
6. Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press.
7. Clough, J. (2015). *Principles of Cybercrime*. Cambridge University Press.

8. Rustambayev M.H. (2021). *O‘zbekiston Respublikasi Jinoyat huquqi kursi*. Maxsus qism. Toshkent: Daryo-Press.
9. Ziyayev M. (2023). *Raqamli makonda jinoyatlarni tergov qilish metodikasi*. Monografiya. Toshkent: TDYU nashriyoti.
10. INTERPOL. (2023). *Global Cybercrime Threat Assessment Report*. Lyon: INTERPOL General Secretariat.
11. European Union Agency for Cybersecurity (ENISA). (2023). *ENISA Threat Landscape 2023*.
12. Galiyev R. (2022). "Kiberjinoyatchilikka qarshi kurashishda yurisdiksiya muammolari va xalqaro tajriba". *Huquq va burch*, №4, 45-52-b.