KIBERMAKONDA FIRIBGARLIK JINOYATLARIGA QARSHI KURASHISHNI TAKOMILLASHTIRISH

IMPROVING THE FIGHT AGAINST FRAUD IN CYBERSPACE

СОВЕРШЕНСТВОВАНИЕ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСКИМ ПРЕСТУПЛЕНИЯМ В КИБЕРПРОСТРАНСТВЕ

Abdujalilov Shaxboz Jahongir o‘g‘li
(O‘zbekiston Respublikasi IIV Akademiyasi kursanti)
Iminov Abdurasul Abdulatipovich
(O‘zbekiston Respublikasi IIV Akademiyasi Raqamli texnologiyalar va axborot xavfsizligi kafedrasi boshlig‘i)

Annotatsiya: Ushbu maqolada bugungi global raqamli ekotizimda kiberjinoyatlarning texnologik transformatsiyasi, ularning rivojlanish tendensiyalari hamda jamiyat hayotining turli jabhalariga o‘tkazayotgan ko‘p qirrali salbiy oqibatlari tahlil qilinadi. Zamonaviy kibertahdidlar shunchaki texnik hodisa yoki oddiy dasturiy hujum bo‘lmay, balki geosiyosiy, huquqiy, ijtimoiy va iqtisodiy miqyosda chuqur asoratlarni yuzaga keltiruvchi murakkab tizimga aylanganligi asoslab berilgan. Ushbu maqolada raqamli texnologiyalar rivojlanishi sharoitida kibermakonda sodir etilayotgan firibgarlik jinoyatlariga qarshi kurashishning huquqiy va institutsional mexanizmlarini takomillashtirish masalalari tahlil qilinadi. Muallif milliy qonunchilik va xalqaro huquqiy normalarni, xususan, Kiberjinoyatchilik bo‘yicha Budapesht konvensiyasi prinsiplarini qiyosiy o‘rgangan holda, kiberfiribgarlikning zamonaviy usullari va ularning malakalanish muammolarini yoritib beradi. Tadqiqot davomida jinoyat qonunchiligini liberallashtirish va raqamli makonda xavfsizlikni ta’minlash muvozanatini saqlash, shuningdek, huquqni muhofaza qiluvchi organlarning texnik salohiyatini oshirish bo‘yicha ilmiy-amaliy taklif va tavsiyalar ishlab chiqilgan.

Kalit so‘zlar: Kiberjinoyat, kibermakon, kiberxavfsizlik, raqamli tahdidlar, Kibermakonda firibgarlik, kiberjinoyatchilik, huquqiy normalar, jinoyat qonunchiligi, raqamli xavfsizlik, Budapesht konvensiyasi, kiberhudud, axborot texnologiyalari.

Abstract: This article analyzes the technological transformation of cybercrime and its development trends within today's global digital ecosystem, as well as the issues of improving legal and institutional mechanisms to combat fraudulent crimes committed in cyberspace. It is substantiated that modern cyber threats are no longer merely technical phenomena, but have evolved into complex systems causing profound

geopolitical, legal, and economic consequences. By conducting a comparative study of national legislation and international legal norms, particularly the principles of the Budapest Convention on Cybercrime, the author highlights modern methods of cyber-fraud and the challenges associated with their legal qualification. Conclusively, the research formulates scientific and practical proposals aimed at balancing the liberalization of criminal law with ensuring security in the digital space, alongside enhancing the technical and personnel capacity of law enforcement agencies.

Keywords: Cybercrime, cyberspace, cybersecurity, digital threats, Cybercrime, cyberspace, cyber-fraud, digital security, cyber threats, legal norms, criminal legislation, Budapest Convention, digital ecosystem, institutional mechanisms.

Аннотация: В данной статье анализируются технологическая трансформация киберпреступности в современной глобальной цифровой экосистеме, тенденции её развития и многоаспектное негативное влияние на различные сферы жизни общества. В данной статье анализируются технологическая трансформация киберпреступности и тенденции ее развития в условиях современной глобальной цифровой экосистемы, а также вопросы совершенствования правовых и институциональных механизмов борьбы с мошенническими преступлениями, совершаемыми в киберпространстве. Обосновано, что современные киберугрозы стали сложной системой, влекущей за собой глубокие последствия на геополитическом, правовом и экономическом уровнях, выходя за рамки обычных технических инцидентов. На основе сравнительного изучения национального законодательства и международных правовых норм, в частности принципов Будапештской конвенции о киберпреступности, автор освещает современные методы кибермошенничества и проблемы их правовой квалификации. В заключении исследования сформулированы научно-практические предложения и рекомендации, направленные на соблюдение баланса между либерализацией уголовного законодательства и обеспечением безопасности в цифровом пространстве, а также на повышение технического и кадрового потенциала правоохранительных органов.

Ключевые слова: Киберпреступность, киберпространство, кибербезопасность, цифровые угрозы, Киберпреступность, киберпространство, кибермошенничество, цифровая безопасность, киберугрозы, правовые нормы, уголовное законодательство, Будапештская конвенция, цифровая экосистема, институциональные механизмы.

Kirish

Insoniyat sivilizatsiyasining bugungi bosqichi global raqamli ekotizimning shiddatli rivojlanishi va hayotning barcha jabhalariga axborot texnologiyalarining

integratsiyalashuvi bilan tavsiflanadi. To‘rtinchi sanoat inqilobi (Industry 4.0) nafaqat iqtisodiy o‘sish va ijtimoiy qulayliklarni ta’minladi, balki an’anaviy jinoyatchilik shakllarining ham transformatsiyaga uchrashiga zamin yaratdi. Bugungi kunda jinoyat olamining eng xavfli va dinamik rivojlanayotgan tarmoqlaridan biri bu – kibermakondagi firibgarlikdir.

Kibermakon o‘zining anonimligi, transchegaraviy tabiati va jismoniy chegaralarning yo‘qligi bilan jinoyatchilar uchun juda qulay muhit hisoblanadi. Agarda ilgari firibgarlik harakatlari bevosita shaxsiy muloqot yoki qog‘oz hujjatlarni qalbakilashtirish orqali sodir etilgan bo‘lsa, bugungi kunda ijtimoiy muhandislik (social engineering), fishing (phishing), fishing hujumlari va sun’iy intellekt (deepfake) texnologiyalari yordamida amalga oshirilmoqda. Bu esa milliy va xalqaro miqyosda huquqiy mexanizmlarni tubdan qayta ko‘rib chiqishni va takomillashtirishni taqozo etadi.

I. Kiberjinoyatlarning Texnologik Transformatsiyasi va Rivojlanish Tendensiyalari

Zamonaviy kibertahdidlar shunchaki oddiy dasturiy hujum yoki texnik hodisa doirasidan chiqib ketgan. Ular bugungi kunda geosiyosiy, huquqiy, ijtimoiy va iqtisodiy miqyosda tizimli asoratlarni keltirib chiqaruvchi murakkab kiber-industriyaga aylandi. Kiberfiribgarlikning transformatsiyasini quyidagi asosiy tendensiyalarda ko‘rish mumkin:

1.1. Ijtimoiy muhandislik va Fishingning evolyutsiyasi

Hozirgi kunda kiberfiribgarlikning qariyb 90 foizi inson omili, ya’ni ijtimoiy muhandislik usullari bilan bog‘liq. Jinoyatchilar jabrlanuvchining psixologik holatini, qo‘rquv, qiziqish yoki ishonch tuyg‘ularini manipulyatsiya qilish orqali bank plastik kartalari ma’lumotlarini yoki maxfiy parollarni qo‘lga kiritadilar. SMS-vishing (smishing) va ovozli fishing (vishing) orqali bank tizimi xodimlari niqobi ostida qo‘ng‘iroq qilish holatlari global muammoga aylandi.

1.2. Sun’iy intellekt va Deepfake texnologiyalari

2020-yillarning o‘rtalariga kelib, kiberfiribgarlikda neyrotarmoqlar va sun’iy intellektdan foydalanish misli ko‘rilmagan darajada o‘sdi. Generativ sun’iy intellekt yordamida haqiqiy shaxslarning ovozi va videosini (Deepfake) o‘xshatib yaratish orqali kompaniya rahbarlari yoki yaqin qarindoshlar nomidan pul mablag‘larini o‘zlashtirish holatlari ko‘paymoqda. Bu esa an’anaviy biometrik himoya tizimlarining ham zaifligini ko‘rsatib qo‘ydi.

1.3. Kriptovalutalar va Anonim moliyaviy oqimlar

Kiberfiribgarlik orqali qo‘lga kiritilgan mablag‘larni legallashtirish (yuvish) jarayoni ham raqamlashdi. Kriptoaktivlar va blokcheyn texnologiyasi an’anaviy bank nazoratidan chetga chiqish imkonini beradi. “Mikserlar” deb ataluvchi platformalar

orqali pullarning izini yo‘qotish huquqni muhofaza qiluvchi organlar uchun tergov jarayonini murakkablashtirmoqda.

II. Kibermakonda Firibgarlikka Qarshi Kurashishning Huquqiy va Institutsional Muammolari

Kiberfiribgarlikka qarshi kurashishda milliy va xalqaro huquq normalari o‘rtasida jiddiy nomutanosibliklar mavjud. Ushbu muammolarni bir nechta tizimli bloklarga ajratish mumkin:

2.1. Yurisdiksiya va Transchegaraviylik muammosi

Kiberjinoyatchilik hudud tanlamaydi. Jinoyatchi O‘zbekiston fuqarosining mablag‘ini AQShda joylashgan server orqali, Janubiy-Sharqiy Osiyo davlatlaridan turib o‘g‘irlashi mumkin. Bunday holatda milliy huquqni muhofaza qiluvchi organlarning vakolati o‘z davlati hududi bilan cheklanadi. Xalqaro huquqiy yordam ko‘rsatish to‘g‘risidagi shartnomalar esa byurokratik jarayonlardan iborat bo‘lib, kiberjinoyatlarning tezkor tabiati (pullar soniyalar ichida ko‘chiriladi) bilan mos kelmaydi.

2.2. Raqamli dalillarni olish va baholash muammolari

Jinoyat-protsessual qonunchiligida raqamli (elektron) dalillar tushunchasi, ularni olib qo‘yish, ko‘zdan kechirish va saqlash tartibi hali ham to‘liq mukammallikka erishmagan. IP-manzillar, log-fayllar va elektron hamyonlar hisobotlari raqamli dalil sifatida oson o‘zgartirilishi yoki yo‘q qilinishi mumkinligi sababli, ularning autentifikatsiyasini sud jarayonida isbotlash qiyinchilik tug‘diradi.

III. Xalqaro Tajriba: Budapesht Konvensiyasi va Rivojlangan Davlatlar amaliyoti

Kibermakonda firibgarlikka qarshi kurashishda xalqaro standartlarni o‘rganish milliy qonunchilikni takomillashtirishning bosh mezoni hisoblanadi.

3.1. Kiberjinoyatchilik bo‘yicha Budapesht konvensiyasi (2001)

Ushbu hujjat kiberjinoyatlarga qarshi kurashish bo‘yicha yagona va eng fundamental global platformadir. Konvensiyaning asosiy maqsadi:

Milliy moddiy huquq normalarini uyg‘unlashtirish (kiberfiribgarlik, kompyuter tizimlariga noqonuniy kirishni kriminallashtirish).

Protsessual huquq vositalarini (ma’lumotlarni zudlik bilan saqlab qo‘yish, tarmoq-trafikini kuzatish) belgilash.

Tezkor xalqaro hamkorlik, jumladan, 24/7 rejimida ishlaydigan aloqa tarmoqlarini tashkil etish.

O‘zbekiston Respublikasining ushbu konvensiya prinsiplariga bosqichma-bosqich integratsiyalashuvi global miqyosda tezkor axborot almashish imkonini beradi.

3.2. AQSh va Yevropa Ittifoqi tajribasi

AQShda Federal tergov bürosi (FTB) qoshida IC3 (Internet Crime Complaint Center) markazi faoliyat yuritadi. Har qanday fuqaro kiberfiribgarlikka duch kelganda

ushbu platformaga onlayn ariza beradi va banklar bilan hamkorlikda mablag‘larni zudlik bilan bloklash (Kill Chain) mexanizmi ishga tushadi. Yevropa Ittifoqida esa Europol qoshidagi Yevropa kiberjinoyatchilik markazi (EC3) davlatlararo muvofiqlashtirishni ta’minlaydi.

IV. O‘zbekiston Respublikasi Qonunchiligini Takomillashtirish Bo‘yicha Taklif va Tavsiyalar

O‘zbekiston Respublikasi Jinoyat kodeksining 168-moddasi (Firibgarlik) axborot texnologiyalaridan foydalanib sodir etilgan qilmishlar uchun javobgarlikni ko‘zda tutadi. Shuningdek, "Kiberxavfsizlik to‘g‘risida"gi Qonun qabul qilingan. Biroq, amaliyot samaradorligini oshirish uchun quyidagi islohotlarni amalga oshirish zarur:

4.1. Jinoyat va Jinoyat-protsessual kodekslariga o‘zgartirishlar kiritish

Raqamli dalillarning huquqiy maqomi: JPKga elektron dalillarni protsessual rasmiylashtirishning soddalashtirilgan, ammo xavfsiz mexanizmini kiritish.

Sanksiyalarni differensiallash: Sun’iy intellekt va deepfake yordamida sodir etilgan kiberfiribgarlikni og‘irlashtiruvchi holat sifatida belgilash.

4.2. Institutsional mexanizmlarni optimallashtirish

Yagona Kiber-vasiylik (Cyber-anti-fraud) tizimi: Markaziy bank, tijorat banklari va Huquqni muhofaza qiluvchi organlar o‘rtasida firibgarlik tranzaksiyalarini real vaqt rejimida (real-time) aniqlash va 30 daqiqa ichida muzlatish imkonini beruvchi integratsiyalashgan antifraud tizimini joriy etish.

Kadrlar salohiyati: Prokuratura, ichki ishlar va sud organlarida "Raqamli kriminalistika" (Digital Forensics) bo‘yicha ixtisoslashgan maxsus kadrlar tayyorlash tizimini kengaytirish.

Xulosa

Kibermakonda firibgarlik jinoyatlariga qarshi kurashish faqatgina jazo choralarini kuchaytirish bilan cheklanmaydi. Bu muammo huquqiy normalarni texnologik taraqqiyot bilan uyg‘unlashtirish, xalqaro hamkorlikni (Budapesht konvensiyasi doirasida) jadallashtirish va jamiyatda "kiber-gigiyena" madaniyatini yuksaltirish orqali tizimli yondashuvni talab etadi. Taklif etilayotgan huquqiy va institutsional mexanizmlarning joriy etilishi davlatimiz iqtisodiy xavfsizligini hamda fuqarolarning raqamli makondagi huquqlari himoyasini yangi bosqichga olib chiqadi.

Foydalanilgan Adabiyotlar Ro‘yxati

1.O‘zbekiston Respublikasining Jinoyat kodeksi. – Toshkent: Adolat, 2025.

2.O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonunu, 05.04.2022 yildagi O‘RQ-764-son.

3.Convention on Cybercrime (Budapest Convention), ETS No. 185, Council of Europe, 2001.

4.Rustambayev M.X. O‘zbekiston Respublikasi Jinoyat huquqi kursi. III tom: Maxsus qism. – Toshkent: Ilm-ziyo, 2021.

5.Brenner, S. W. (2024). Cybercrime: Criminal Threats from Cyberspace. ABC-CLIO.

6.Interpol. (2025). Global Cybercrime Results and Trends Report. Lyon: Interpol Assessment.

7. Markaziy bank tahliliy hisobotlari: Bank tizimida axborot xavfsizligi holati (2024–2025-yy.).