ZAMONAVIY KIBERJINOYATCHILIK: UNING TRANSCHEGARAVIY XUSUSIYATLARI, OQIBATLARI VA UNGA QARSHI KURASHISHDA AMALIY TAKLIFLAR

IIV Akademiyasi Raqamli texnologiyalar va axborot xavfsizligi kafedrasi boshlig‘i, fizika matematika fanlari nomzodi dotsent ***A.A.Iminov***
IIV Akademiyasi kunduzgi ta’lim 3-bosqich 333-guruh kursanti safdor
Patidinov Saidislom Xusanboy o‘g‘li

Annotatsiya

Ushbu maqolada global tarmoqda axborot texnologiyalaridan foydalangan holda sodir etilayotgan kiberjinoyatchilikning ijtimoiy-huquqiy tabiati va uning turlari tahlil qilinadi. Maqolada kiberjinoyatlarning transchegaraviy xususiyati, an’anaviy jinoyatlardan farqi va jamiyatga yetkazayotgan iqtisodiy-ma’naviy zararlari yoritilgan. Eng muhimi, maqolada kiberjinoyatchilikning oldini olish, raqamli dalillarni yig‘ish mexanizmlarini takomillashtirish hamda ushbu xavfga qarshi kurashish samaradorligini oshirish bo‘yicha aniq qonunchilik va amaliy takliflar ilgari surilgan.

Kalit so‘zlar Kiberjinoyatchilik, xakerlik, raqamli firgarlik, transchegaraviy jinoyat, profilaktika, raqamli dalil, kiber-kriminalistika, qonunchilikni takomillashtirish, kiber-patrul.

Kirish

Bugungi kunda axborot-kommunikatsiya texnologiyalarining shiddatli rivojlanishi nafaqat hayotimizni qulaylashtirdi, balki jinoiy dunyo uchun ham yangi platforma yaratdi. Kiberjinoyatchilik — an’anaviy jinoyatchilik chegaralarini buzib o‘tib, hudud yoki makon tanlamaydigan global xavfga aylandi. Bugun kiberjinoyatchilar yirik moliyaviy korxonalardan tortib, oddiy fuqarolarning shaxsiy jamg‘armalarigacha maqsadli hujumlar uyushtirmoqda. Ushbu tahdidga qarshi faqat mudofaa bilan emas, balki jinoyatning tub ildizini yo‘qotish va tizimli profilaktika orqali kurashish davr talabidir.

Kiberjinoyatchilikning Asosiy Ko‘rinishlari

Kiberjinoyatchilikni shartli ravishda bir nechta yirik guruhlarga ajratish mumkin:

1. **Iqtisodiy va Moliyaviy Kiberjinoyatlar:** Plastik kartalardagi mablag‘larni yashirin talon-taroj qilish, fishing (soxta havolalar) orqali bank ma’lumotlarini o‘g‘irlash va internet-firgarlik.

2. **Tizimli Kiberjinoyatlar (Xakerlik):** Davlat va xususiy korxonalarning serverlariga ruxsatsiz kirish, ma’lumotlar bazasini o‘g‘irlash yoki ularni o‘chirib yuborish bilan tahdid qilib pul talab qilish (Ransomware).
3. **Ijtimoiy va Ma’naviy Jinoyatlar:** Internet tarmog‘ida shaxsning qadr-qimmatini kamsitish (kiberbulling), tuhmat tarqatish, firgarlik maqsadida birovning shaxsiyatini o‘g‘irlash (soxta profillar yaratish).

Kiberjinoyatchilikning Oldini Olish Bo‘yicha Chora-Tadbirlar

Kiberjinoyatchilik an’anaviy jinoyatlardan o‘zining yashirinligi (anonimligi) bilan ajralib turadi. Shu sababli uni sodir etilgandan keyin fosh etishdan ko‘ra, oldini olish choralarini kuchaytirish zarur:

Bank va Moliya Tizimlarida Filtrlar O'rnatish: Bank ilovalarida shubhali va bir vaqtning o‘zida bir nechta hisob raqamlarga yirik mablag‘ o‘tkazmalarini avtomatik ravishda vaqtincha bloklovchi "Anti-frood" (firgarlikka qarshi) aqlli tizimlarini joriy etish. **Aholining Huquqiy va Raqamli Savodxonligini Oshirish:** Ayniqsa yoshlar va qariyalar o‘rtasida kiber-firgarlarning tuzoqlariga tushib qolmaslik bo‘yicha mahalla va ta’lim muassasalarida doimiy tushuntirish ishlarini olib borish. **Provayderlar Bilan Tezkor Hamkorlik:** Internet xizmatini ko‘rsatuvchi provayderlar va mobil operatorlar tomonidan firgarlik saytlari va soxta SMS-jo‘natmalarni tarmoq darajasidayoq aniqlab, bloklash mexanizmini yo‘lga qo‘yish.

Kiberjinoyatchilikka Qarshi Kurashishni Takomillashtirish Bo‘yicha AMALIY TAKLIFLAR

Maqolaning asosiy ilmiy yangiligi sifatida kiberjinoyatchilik darajasini keskin kamaytirishga qaratilgan quyidagi **strategik takliflar** ilgari suriladi:

1. **"Kiber-patrul" (Cyber Patrol) Tizimini Tashkil Etish:** Huquqni muhofaza qiluvchi organlar tarkibida faqat ijtimoiy tarmoqlar, messenjerlar (Telegram, WhatsApp va h.k.) va "Darknet" tarmoqlarida firgarlik, taqiqlangan moddalar savdosi hamda xakerlik forumlarini doimiy monitoring qiluvchi va jinoyatni rejalashtirish bosqichidayoq aniqlovchi maxsus virtual patrul bo‘linmalarini kengaytirish.
2. **Raqamli Dalillar To‘g‘risidagi Qonunchilikni Integratsiya Qilish:** Jinoyat-prosessual qonunchiligiga "Raqamli dalil" (skrinshotlar, IP-manzillar loglari, blokcheyn tranzaksiyalari) tushunchasini aniq huquqiy maqomini kiritish va ularni sud jarayonida rasmiy dalil sifatida qabul qilish tartibini soddalashtirish.
3. **Kiber-kriminalistika (Digital Forensics) Markazlarini Rivojlantirish:** Kiberjinoyatchilar o‘z izlarini o‘chirish uchun VPN, proksi va

anonimizatorlardan foydalanishadi. Ularni fosh etish uchun eng zamonaviy texnik laboratoriyalar va kriptovalyuta oqimlarini kuzatuvchi dasturiy majmualarni sotib olish va mutaxassislar tayyorlash.

4. **Transchegaraviy Tezkor Aloqa Platformasini Yaratish:** Kiberjinoyatchi ko‘p hollarda boshqa davlatda turib jinoyat sodir etadi. Shuning uchun xorijiy davlatlar huquqni muhofaza qiluvchi organlari bilan byurokratik xatlarsiz, bir necha daqiqa ichida jinoyatchining IP-manzilini va joylashgan joyini aniqlash imkonini beruvchi **tezkor transchegaraviy aloqa tarmog‘ini** tashkil etish lozim.

Xulosa

Kiberjinoyatchilik bugungi kunning eng tez o‘zgaruvchan va xavfli jinoiy faoliyatlaridan biridir. Unga qarshi eski uslublar bilan kurashib bo‘lmaydi. Taklif etilayotgan "Kiber-patrul" tizimi, qonunchilikdagi raqamli islohotlar va xalqaro tezkor hamkorlik platformasi kiberjinoyatchilikni jilovlashda va fuqarolarning raqamli makondagi xavfsizligini ta’minlashda hal qiluvchi burilish nuqtasi bo‘la oladi.

Foydalanilgan Adabiyotlar (References)

1. **Brenner, S. W.** (2010). *Cybercrime: Criminal Threats from Cyberspace*. ABC-CLIO.
2. **Casey, E.** (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press.
3. **Rustambayev, M. H.** (2023). *O‘zbekiston Respublikasining Jinoyat huquqi (Maxsus qism)*. Toshkent: Yuridik adabiyotlar nashriyoti. (Axborot texnologiyalari sohasidagi jinoyatlar bobi).
4. **UNODC (United Nations Office on Drugs and Crime).** (2021). *Comprehensive Study on Cybercrime*. UN Official Reports.