

KIBERJINOYATLAR VA ULARNI TERGOV QILISHDA ZAMONAVIY TERGOVCHI QIYOFASI.

O'rolova Nozima Erkin qizi

*Huquqni muhofaza qilish akademiyasi "Prokurorlik faoliyati" yo'nalishi 2-kurs
talabasi E-mail: urolovanozima5@gmail.com*

Annotatsiya: *Mazkur maqolada kiberjinoyatlarni tergov qilishda zamonaviy tergovchining qiyofasi, uning kasbiy bilim va ko'nikmalariga oid masalalar tahlil qilingan.*

Kalit so'zlar: *kiberjinoyatlar, tergovchi, tergov, kiberxavfsizlik, zamonaviy raqamli texnologiyalar.*

Аннотация: *В статье анализируется образ современного следователя, его профессиональные знания и умения в расследовании киберпреступлений.*

Ключевые слова: *киберпреступления, следователь, расследование, кибербезопасность, современные цифровые технологии.*

Abstract: *This article analyzes the image of a modern investigator, his professional knowledge and skills in investigating cybercrimes.*

Keywords: *cybercrimes, investigator, investigation, cybersecurity, modern digital technologies.*

Hozirda hayotimizni zamonaviy raqamli texnologiyalar imkoniyatlaridan foydalanmasdan o'tkazishni tasavvur qilishimiz qiyin. Lekin ba'zi bir toifa insonlar borki, raqamli texnologiyalar beradigan imkoniyatlardan g'ayrihuquqiy va g'ayriijtimoiy maqsadlarda, boshqalardan firibgarlik orqali pul undirish, shaxslarning bank hisobvaraqlaridagi pullarni yechib olish, tarmoqlarda taqiqlangan materiallarni tarqatish va shu kabi bir qancha noqonuniy qilimishlarni sodir etish maqsadida foydalanadilar. Zamonaviy axborot texnologiyalari bilan sodir etilgan jinoyatlarni umumiy nom bilan kiberjinoyatlar deb ataymiz. Kiberjinoyatlar bu kompyuterlar, tarmoqlar yoki raqamli qurilmalardan foydalanib amalga oshiriladigan jinoyatlardir. Bugungi kunda kiberjinoyatlar zamonaviy dunyoda eng ko'p sodir bo'layotgan va insoniyat xavfsizligiga xavf solayotgan jinoyatlarning bir turidir. Bu turdagi jinoyatlarga qarshi kurashish hozirda butun dunyoda dolzarb ahamiyat kasb etadi. Kiberjinoyatlarni sodir qilish uchun shaxs jinoyat sodir etish joyiga borishi shart emas, u o'z xonasida turib ham o'zining g'arazli maqsadini amalga oshirishi, kiberjinoyatlarning chegara tanlamasligini bildiradi. Aynan shuning uchun ham davlatlar o'zaro hamkorlikda kiberjinoyatchilikka qarshi kurashish choralarini ko'rish lozim deb bilamiz.

Kiberjinoyatchilik tushunchasini yanada yaxshiroq tushunishimiz uchun ushbu tushunchaga oid xalqaro va milliy qonunchiligimizdagi normalarga to'xtalib

o'tishimiz darkor. Kiberjinoyatchilikka qarshi kurash yuzasidan 2001-yil 23-noyabrda Yevropa Kengashi tomonidan "Kiberjinoyatchilikka qarshi kurashish konvensiyasi" qabul qilingan.¹ Ushbu konvensiyada kiberjinoyatchilikka aniq ta'rif berilmagan bo'lsada, kompyuter tizimlariga noqonuniy kirish (unauthorized access), kompyuter ma'lumotlariga noqonuniy kirish yoki ularni buzish (data interference), kompyuter tizimining ishlashiga noqonuniy ta'sir ko'rsatish (system interference), ma'lumotlarni ushlab qolish yoki eshitish (illegal interception), kompyuterga oid firibgarlik va soxtalashtirish (computer-related fraud and forgery) kabi tushunchalarga to'xtalib o'tilgan. Milliy qonunchiligimizda esa kiberjinoyatchilik axborotni egallash, uni o'zgartirish, yo'q qilish yoki axborot tizimlari va resurslarini ishdan chiqarish maqsadida kibermakonda dasturiy ta'minot va texnik vositalardan foydalanilgan holda amalga oshiriladigan jinoyatlar yig'indisi deb belgilangan.²

Kiberjinoyatchilikka qarshi kurashishda kiberxavfsizlik tizimlarini takomillashtirish bugungi kunning dolzarb masalalaridandir. Dunyoda ko'plab mamlakatlarda kiberjinoyatchilikka qarshi kurashishning maxsus tizimlari faoliyat olib boradi. Amerika Qo'shma Shtatlari, Buyuk Britaniya, Germaniya, Fransiya, Rossiya va Xitoy kabi mamlakatlarda kiberjinoyatchilikka qarshi kurashish uchun maxsus tuzilmalar o'z faoliyatini olib boradi. Amerika Qo'shma Shtatlarida kiberjinoyatchilikka qarshi kurashish bo'yicha Federal tergov byurosining kiberjinoyatlarga qarshi bo'limi (FBI Cyber Division) ish olib boradi.³ Buyuk Britaniyada kiberxavfsizlikni ta'minlaydigan markaz (National Cyber Security Centre), Rossiya Federatsiyasida Federal xavfsizlik xizmati (ФСБ), Xitoy xalq Respublikasida davlat xavfsizligi vazirligi (Ministry of State Security), Germaniya Federativ Respublikasida Axborot xavfsizligi federal idorasi (Federal Office for Information Security), Fransiya axborot tizimlarining xavfsizligini ta'minlovchi agentlik (Agence nationale de la sécurité des systèmes d'information) faoliyat olib boradi. Mamlakatimizda kiberxavfsizlik sohasida vakolatli davlat organi Davlat xavfsizlik xizmati hisoblanadi.

Kiberjinoyatlar bilan bog'liq statistikani tahlil qiladigan bo'lsak, 2023 yilning 11 oyida 5, 5 mingta kiberjinoyat sodir etilgan. Shundan 70 foizi bank kartalari bilan bog'liq firibgarlik va o'g'irlik jinoyatlari hisoblanadi.⁴ Xalqaro maydonda ham kiberjinoyatchilik mamlakatlar iqtisodiyoti uchun katta zarar keltirmoqda.

Bugungi kunga kelib ilmiy soha vakillari, amaliyotchi xodimlar tomonidan O'zbekistonda kiberjinoyatchilik ko'rsatkichlari 2-3 barobarga ko'payganligi ta'kidlanmoqda.

Kiberjinoyatchilikka qarshi kurashishda nafaqat huquqni muhofaza qiluvchi organlar faoliyatining samaradorligi oshirish, balki fuqarolarning ham

¹ <https://www.unodc.org/unodc/en/cybercrime/convention/home.html>

² <https://lex.uz/uz/docs/-5960604> "Kiberxavfsizlik to'g'risida"gi O'zbekiston Respublikasi Qonuni

³ <https://www.fbi.gov/investigate/cyber>

⁴ <https://www.kun.uz/news/2023/12/20/ozbekistonda-2023-yilda-55-mingta-kiberjinoyat-sodir-etildi>

kiberhujumlarga qarshi ogohligini oshirish kerak. Internetdan foydalanuvchi har bir shaxs axborotmakonda vujudga keladigan kiber tahdidlarga qarshi immunitetni o'zida shakllantirishi kerak.

Zamonaviy raqamli texnologiyalar rivojlanib borgan sari axborot makonda sodir etiladigan jinoyatlarning turlari va toifalari ham ko'payib bormoqda. Oldinlari real hayotda sodir etiladigan ba'zi bir jinoyat toifalari bugungi kunda virtual ko'rinishga o'tgan. Bunga misol qilib giyohvandlik vositalari, psixotrop moddalar sotish, pornografik materiallar tarqatish, axborot texnologiyalaridan foydalanib o'g'rilik, firibgarlik jinoyatlarini bugungi kunda kibermakonga ko'chganligini ta'kidlab o'tishimiz lozim. Endilikda jinoyatchilar kibermakonda ko'chgan ekan, bu sohada tergovchilar ham kibermakonda ulardan kam bo'lmagan ko'nikmalarga ega bo'lishi kerak. Kibermakonda jinoyatlarni aniqlash, ochish va fosh qilish uchun tergovchi o'zida qanday ko'nikmalarni shakllantirishi kerak degan savol vujudga kelishi o'rinli. Kiberjinoyatlarni tergov qiladigan tergovchi ham huquqshunos ham texnolog bo'lishi lozim. Bu biz yashab turgan davrimizning dolzarb talabiga aylanib bormoqda.

Kiberjinoyatlarni tergov qilishda tergovchi uchun muhim ko'nikmalardan biri texnikaga oid bilim va ko'nikmalarga ega bo'lish zarurati. Tergovchi raqamli texnologiyalar, axborot tizimlari, operatsion tizimlar asoslarini tushunishi va ular bilan mustaqil ishlay olishi, axborot tizimlaridan raqamli dalillarni olish va ular bilan ishlash, shifrlangan ma'lumotlar va fayllar bilan ishlash, zararkunanda dasturlarni aniqlash bilan bog'liq texnik bilimlarga ega bo'lishi kerak.

Ikkinchi muhim xususiyat esa analitik ko'nikmalar va axborot izlash kompetensiyasining rivojlanganligi. Bunda urg'u asosan raqamli tahliliy ko'nikmalar, kiberjinoyatlarni aniqlash va izlash ko'nikmalariga qaratilishi lozim.

Keyingisi tahliliy fikrlash, sinchkovlik, mas'uliyat kabi shaxsiy ko'nikmalarga (soft skills) ega bo'lishi lozim. Yuqoridagi ko'nikmalar bilan birgalikda tergovchida yuqori saviyada huquqiy bilim ham bo'lishi lozim. Kiberjinoyatlarni tergov qilishda tergovchi nafaqat milliy qonunchilikni yaxshi bilishi balki xalqaro qonun normalarini ham yaxshi o'zlashtirgan bo'lishi lozim. Kiberjinoyatlar chegaralab bo'lmaydigan, transmilliy jinoyatlarga ham aylanib ketishi mumkin.

Kiberjinoyatlarni tergov qilish- bu murakkab, tergovchidan yuqori saviyadagi zamonaviy raqamli texnologiyalar bilan ishlash ko'nikmasini talab qiladigan soha hisoblanadi. Bunda tergovchining raqamli texnologiyalarga oid bilimlar, huquqiy bilimlar va kuchli tahliliy ko'nikmalarga ega bo'lishi muhim ahamiyat kasb etadi.

Xulosa qilib aytadigan bo'lsak, bugungi kunda kiberjinoyatlarni tergov qilishda zamonaviy tergovchi quyidagi ko'nikmalarga ega bo'lishi kerak deb hisoblaymiz:

- zamonaviy raqamli texnologiyalarni tushunish
- tahliliy fikrlash
- yuqori saviyada huquqiy bilimlarga ega bo'lish
- axborot xavfsizligini saqlash

- xalqaro miqyosda hamkorlik qilish

So'nggi vaqtlarda kiberjinoyatlar ko'lami kengayib borar ekan, bu toifadagi jinoyatlarga qarshi kurashish, ularni aniqlash va tergov qilish yuzasidan murakkab yondashuvlarni talab qilmoqda. Doimiy tergov usullari orqali kiberjinoyatlarni tergov qilish o'zining samarasini asta-sekin yo'qotib bormoqda.

Shu sababli kiberjinoyatlarni tergov qilish sohasida alohida ixtisoslashtirilgan tergovchilar bazasini shakllantirish lozim deb hisoblaymiz. Bu ixtisoslikdagi tergovchilar bazasini shakllantirish kiberjinoyatlarga qarshi samarali kurashishda o'zining ijobiy natijasini beradi. Shu yo'nalishda faoliyat olib boruvchi tergovchilar uchun doimiy malaka oshirish kurslari, xalqaro tajriba almashinuvi va ularni zamonaviy texnik jihozlar bilan ta'minlash kabi tizimli chora-tadbirlarni joriy etish muhim ahamiyatga ega. Ixtisoslashtirilgan tergovchilar bazasini shakllantirish— nafaqat kiberjinoyatlarga tezkor va samarali kurashishni ta'minlaydi, balki milliy axborot xavfsizligini mustahkamlash yo'lida ham muhim qadam bo'lib xizmat qiladi.

IQTIBOSLAR:

1. Convention on Cybercrime
<https://www.unodc.org/unodc/en/cybercrime/convention/home.html>
2. “Kiberxavfsizlik to'g'risida”gi O'zbekiston Respublikasi Qonuni
<https://lex.uz/uz/docs/-5960604>
3. <https://www.fbi.gov/investigate/cyber>
4. Internet ma'lumoti: <https://www.kun.uz/news/2023/12/20>