KIBERJINOYATLAR PROFILAKTIKASINI TAKOMILLASHTIRISHNING AYRIM MASALALARI

Isroilov Odiljon Oqiljonovich
O‘zbekiston Respublikasi Ichki ishlar vazirligi akademiyasi kursanti

https://doi.org/ 10.5281/zenodo.23497037

Annotatsiya: Ushbu ilmiy maqolada zamonaviy axborot-kommunikatsiya texnologiyalari jadal rivojlanayotgan sharoitda kiberjinoyatchilikning oldini olish, kiberprofilaktika tizimining nazariy-huquqiy asoslari hamda uning kriminologik mohiyati tahlil qilingan. Kiberjinoyatlarning an’anaviy huquqbuzarliklardan farqli jihatlari, ularning kiberfazodagi dinamikasi hamda profilaktik choralarning ko‘p bosqichli modeli milliy qonunchilik va xalqaro tajriba uyg‘unligida yoritib berilgan.

Kalit so‘zlar: kiberjinoyat, kiberprofilaktika, axborot xavfsizligi, viktimologik profilaktika, raqamli makon, kibergigiyena, huquqbuzarliklar profilaktikasi, kiberxavfsizlik.

Axborot texnologiyalari, raqamli iqtisodiyot va telekommunikatsiya infratuzilmasining keng qamrovli taraqqiyoti jamiyat hayotining barcha sohalarini modernizatsiya qilish bilan bir qatorda, kiberfazoda vujudga kelayotgan yangi xavf-xatarlarning ko‘lamini ham keskin oshirmoqda. Bugungi kunda kiberjinoyatchilik milliy chegaralarni tan olmaydigan, jabrlanuvchilar doirasi keng hamda jamiyat va davlat manfaatlariga jiddiy zarar yetkazuvchi global tahdidga aylandi [1].

Kiberfazoda sodir etilayotgan huquqbuzarliklarga qarshi kurashishda faqatgina sodir etilgan qilmishlarni tergov qilish va jazolash choralariga tayanib qolish o‘z samarasini bermaydi. Chunki kiberjinoyatlarning yuqori darajada yashirin (latent) kechishi, izlarning tezkorlik bilan yo‘qotilishi va aybdorlarning masofadan turib harakat qilishi an’anaviy tergov usullarini murakkablashtiradi. Shu sababli, muammoni bartaraf etishning eng maqbul, iqtisodiy va ijtimoiy jihatdan samarali yo‘li — bu kiberjinoyatchilikning barvaqt profilaktikasini to‘g‘ri va tizimli tashkil etishdir [2].

Kriminologiya va axborot huquqi fanida kiberjinoyatlar profilaktikasi davlat organlari, nodavlat notijorat tashkilotlar, fuqarolik jamiyati institutlari hamda xususiy sektor (banklar, IT-kompaniyalar, aloqa operatorlari) tomonidan kiberfazodagi tahdidlarni aniqlash, bartaraf etish, shuningdek, shaxslarning kiberhujumlar qurboniga aylanishining oldini olishga qaratilgan kompleks chora-tadbirlar majmui sifatida e’tirof etiladi [3].

O‘zbekiston Respublikasining «Huquqbuzarliklar profilaktikasi to‘g‘risida»gi hamda «Kiberxavfsizlik to‘g‘risida»gi Qonunlari normalariga asoslangan holda kiberprofilaktika tizimini quyidagi bosqichlarga ajratish mumkin [4]:

1. Umumiy kiberprofilaktika: Aholining keng qatlamlari orasida kiberxavfsizlik madaniyatini yuksaltirish, kibergigiyena qoidalarini targ‘ib qilish, bank-

moliya tizimi va axborot resurslarining dasturiy-texnik himoyasini kuchaytirish;

2. Maxsus kiberprofilaktika: Zaif axborot tizimlari, muhim axborot infratuzilmasi obyektlari hamda kiberjinoyatchilarning nishoniga aylanish ehtimoli yuqori bo‘lgan sohalar (elektron to‘lov tizimlari, davlat xizmatlari portallari) bo‘yicha yo‘naltirilgan texnik va huquqiy choralarni ko‘rish [5];
3. Yakka tartibdagi (individual) va viktimologik kiberprofilaktika: Ilgari axborot sohasida qonunbuzarlik sodir etgan shaxslar bilan alohida ishlash hamda kiberfiribgarliklar qurboniga aylanishga moyil bo‘lgan toifalar (keksalar, voyaga yetmaganlar, moliyaviy bilimi kam fuqarolar) o‘rtasida maqsadli tushuntirish ishlarini olib borish [6].

Kiberprofilaktikaning samaradorligi davlat va xususiy sektor integratsiyasiga, zamonaviy axborot monitoringi tizimlariga hamda fuqarolarning raqamli savodxonlik darajasiga bevosita bog‘liqdir. Ushbu mexanizmlarni ilmiy-amaliy jihatdan takomillashtirish milliy axborot makonining daxlsizligini ta’minlashning muhim kafolati hisoblanadi.

O‘zbekiston Respublikasida kiberjinoyatchilikning oldini olish va axborot makonida huquqbuzarliklar profilaktikasini tashkil etish bo‘yicha amalga oshirilayotgan amaliy chora-tadbirlar tahlili shuni ko‘rsatadiki, profilaktika xizmatlari va kiberxavfsizlik bo‘linmalari faoliyati kengayib borayotganiga qaramay, sohada qator tizimli to‘siqlar hamda metodologik kamchiliklar saqlanib qolmoqda [7].

Amaliyotda kiberprofilaktika samaradorligiga to‘sqinlik qilayotgan asosiy muammolarni quyidagi yo‘nalishlarga ajratish mumkin:

1. Viktimologik profilaktikaning yetarli darajada yo‘lga qo‘yilmaganligi

Kiberjinoyatlar, xususan, kiberfiribgarlik (fishing, ijtimoiy injiniring, soxta qo‘ng‘iroqlar)ning asosiy omili ko‘p hollarda texnik zaifliklar emas, balki fuqarolarning axborot xavfsizligi madaniyatining pastligidir:

- Raqamli gigiyena va psixologik ishonuvchanlik: Ko‘plab fuqarolar firibgarlarning psixologik manipulatsiyasiga (qo‘rqitish, shoshiltirish, yutuq va’da qilish) aldanib, bank kartasi ma’lumotlari, bir martalik SMS-kodlar va shaxsiy parollarni o‘z ixtiyori bilan taqdim etmoqdalar [8].
- Maqsadli tabaqalanishning yo‘qligi: Profilaktik targ‘ibot tadbirlari ko‘pincha umumiy xarakterga ega bo‘lib, kiberhujumlarga nisbatan eng zaif qatlamlar — keksalar, uy bekalari, talabalar va moliyaviy bilimi past bo‘lgan fuqarolarga alohida moslashtirilgan mexanizmlar asosida yetkazilmayapti.

2. Bank-moliya sektori va huquqni muhofaza qiluvchi organlar o‘rtasidagi profilaktik integratsiyaning sustligi

Kiberjinoyatlarni boshlang‘ich bosqichda to‘xtatib qolishda tezkor axborot almashinuvi hal qiluvchi ahamiyatga ega:

- «Antifrod» (Anti-fraud) tizimlarining to‘liq sinxronlashmaganligi: Tijorat banklari va to‘lov tizimlari o‘rtasida shubhali moliyaviy o‘tkazmalarni (masalan, keksalar hisobidan birdaniga katta summani notanish kartaga o‘tkazish holatlarini) zudlik bilan tahlil qilish va tranzaksiyani profilaktik to‘xtatib turish mexanizmlari barcha muassasalarda bir xil samarali ishlamayapti [9].
- «Drop»-kartalarga qarshi proaktiv nazoratning yetishmasligi: Uchinchi shaxslar (talabalar, ishsizlar) nomiga ochilgan va firibgarlik yo‘li bilan topilgan pullarni yuvishda foydalaniladigan bank kartalari aylanmasini erta bosqichda profilaktik monitoring qilish va bloklash tizimi to‘liq yo‘lga qo‘yilmagan.

3. Sohaviy profilaktika subyektlarining idoraviy tarqoqligi

Kiberprofilaktika faqat ichki ishlar organlarining vazifasi sifatida qabul qilinishi tizimli xatodir:

- Raqamli texnologiyalar vazirligi, Kiberxavfsizlik markazi, Markaziy bank, aloqa operatorlari va ta’lim muassasalari o‘rtasida kiberxavflar to‘g‘risida real vaqt rejimida ogohlantiruvchi yagona profilaktik platformaning mavjud emasligi choralarning samarasini pasaytirmoqda [10].
- Aloqa operatorlari tomonidan soxta (spoofing) raqamlardan kelayotgan xorijiy qo‘ng‘iroqlarni va firibgarlik havolalari mavjud bo‘lgan ommaviy SMS-xabarlarni profilaktik filtrlash mexanizmlari mukammal darajaga yetkazilmagan.

4. Joylardagi profilaktika inspektorlarining kiber-ko‘nikmalari cheklanganligi

Mahallalarda xizmat olib borayotgan profilaktika inspektorlari an’anaviy huquqbuzarliklar bo‘yicha yetarli tajribaga ega bo‘lsa-da, ularning aksariyati kiberjinoyatlarning yangi turlari, raqamli xavfsizlik qoidalari va zamonaviy firibgarlik usullari bo‘yicha aholiga sifatli tushuntirish berish uchun zarur bo‘lgan texnik va metodik tayyorgarlikka ega emas [11].

Ushbu amaliy kamchiliklar kiberjinoyatlar profilaktikasini zamonaviy axborot texnologiyalari, bank integratsiyasi va maqsadli viktimologik yondashuvlar asosida tubdan takomillashtirish zarurligini ko‘rsatadi.

Kiberfazodagi huquqbuzarliklarning o‘sish sur’atini jilovlash va kiberprofilaktika tizimining amaliy samarasini oshirish reaktiv choralardan proaktiv, ya’ni oldindan ogohlantiruvchi va texnologik asoslangan mexanizmlarga o‘tishni taqozo etadi. Mazkur yo‘nalishdagi faoliyatni takomillashtirish maqsadida quyidagi ilmiy-amaliy taklif va tavsiyalar ilgari suriladi

1. Markazlashtirilgan «Milliy antifrod va erta ogohlantirish» platformasini yaratish.

   Markaziy bank, tijorat banklari, to‘lov tizimlari hamda Ichki ishlar vazirligining Kiberxavfsizlik markazini yagona axborot tarmog‘iga

integratsiya qilish zarur. Shubhali, anomaliya sifatida baholangan yoki kiberhujum belgilariga ega bo‘lgan pul o‘tkazmalarini tizim tomonidan 15–30 daqiqaga avtomatik kechiktirish («cooling-off period») va fuqaroga qayta tasdiqlash uchun qo‘ng‘iroq qilish tartibini yo‘lga qo‘yish kiberfiribgarlikning oldini olishda muhim profilaktik to‘siq bo‘ladi [12].

2. «Drop»-kartalar aylanmasiga qarshi profilaktik nazorat va cheklov choralarini kuchaytirish.
   Tijorat banklarida yangi bank kartalarini ochishda xatarlarni baholash tizimini (scoring) kuchaytirish, bir shaxs nomiga asossiz ravishda ko‘plab kartalar ochilishini cheklash hamda talabalar va ijtimoiy himoyaga muhtoj qatlamlar orasida o‘z kartasini uchinchi shaxslarga berishning jinoiy-huquqiy oqibatlarini tushuntiruvchi maqsadli profilaktik tadbirlarni muntazam o‘tkazish lozim.
3. Telekommunikatsiya operatorlari darajasida «Filtrlash va bloklash» mexanizmlarini joriy etish.
   Raqamli texnologiyalar vazirligi va mobil aloqa operatorlari hamkorligida soxta xalqaro raqamlarni (spoofing) almashtirib qo‘ng‘iroq qilish imkonini beruvchi IP-shlyuzlarni tarmoq darajasida avtomatik bloklash tizimini to‘liq ishga tushirish kerak. Shuningdek, fishing havolalarini o‘z ichiga olgan ommaviy SMS-xabarlarni spam-filtrlash algoritmlari orqali zudlik bilan to‘xtatish mexanizmi yo‘lga qo‘yilishi shart [13].
4. Tabaqalashtirilgan viktimologik kiberprofilaktika modelini joriy etish.
   Profilaktik targ‘ibotni aholi toifalariga moslashtirish, jumladan:
   - Keksalar va nafaqaxo‘rlar uchun: Pensiya tarqatish joylari va mahalla markazlarida bank kartasi xavfsizligi bo‘yicha ko‘rgazmali va oddiy tilda tushuntirish ishlarini olib borish;
   - Maktab va oliy o‘quv yurtlarida: «Kibergigiyena va raqamli madaniyat» mavzusida maxsus integratsiyalashgan darslar hamda kiberbulling, fishing va zararli dasturlardan himoyalanish bo‘yicha interfaol treninglar tashkil etish [14].
5. Mahalla profilaktika inspektorlarining kiber-savodxonligini tizimli oshirish.
   IIV Akademiyasi bazasida profilaktika inspektorlari uchun kiberjinoyatlarning zamonaviy turlari, ularning yuzaga kelish mexanizmlari va aholi bilan raqamli profilaktika bo‘yicha muloqot qilish metodikasi yuzasidan qisqa muddatli maxsus malaka oshirish kurslarini joriy etish lozim [15].

Xulosa qilib aytganda, kiberjinoyatchilikka qarshi kurashishning eng samarali yo‘li bu jinoyat oqibatlari bilan kurashish emas, balki uni keltirib chiqaruvchi omillarni oldindan bartaraf etuvchi keng qamrovli kiberprofilaktika tizimini yaratishdir.

Zamonaviy kiberprofilaktika nafaqat huquqiy va ma’muriy choralarni, balki ilg‘or dasturiy-texnik to‘siqlarni (antifrod tizimlari), bank-moliya sektori bilan uzviy integratsiyani hamda fuqarolarning raqamli madaniyatini yuksaltirishni talab etadi. Ushbu chora-tadbirlarning tizimli amalga oshirilishi milliy axborot makonini ishonchli himoya qilish, fuqarolarning shaxsiy va moliyaviy daxlsizligini ta’minlash hamda mamlakatda xavfsiz raqamli muhitni shakllantirishga xizmat qiladi.

REFERENCES:

1. O‘zbekiston Respublikasining «Kiberxavfsizlik to‘g‘risida»gi Qonuni. O‘RQ-764-son. 15.04.2022-y. // Qonunchilik ma’lumotlari milliy bazasi (lex.uz).
2. O‘zbekiston Respublikasining «Huquqbuzarliklar profilaktikasi to‘g‘risida»gi Qonuni. O‘RQ-371-son. 14.05.2014-y. // O‘zbekiston Respublikasi qonun hujjatlari to‘plami. – 2014. – № 20. – 222-m.
3. Maras M.H. Cybercriminology. – Oxford: Oxford University Press, 2016. – 416 p.
4. O‘zbekiston Respublikasi Prezidentining 2021-yil 29-noyabrdagi PF-27-son «O‘zbekiston Respublikasi jamoat xavfsizligi konsepsiyasini tasdiqlash to‘g‘risida»gi Farmoni // Qonunchilik ma’lumotlari milliy bazasi (lex.uz).
5. Clough J. Principles of Cybercrime. 2nd ed. – Cambridge: Cambridge University Press, 2015. – 464 p.
6. Ziyodullayev M.Z., Matchanov A.A. va boshq. Huquqbuzarliklar profilaktikasi: Darslik. – Toshkent: O‘zbekiston Respublikasi IIV Akademiyasi, 2020. – 380 b.
7. Xayitovich, Y. D. (2026). TRANSPORT HUQUQI MUSTAQIL HUQUQ TARMOQI SIFATIDA: NAZARIY ASOSLAR, QIYOSIY TAHLIL VA O‘ZBEKISTON QONUNCHILIGINI TAKOMILLASHTIRISH MASALALARI. Eurasian Journal of Law, Finance and Applied Sciences, 6(2), 67-71.
8. Xayitovich, Y. J. (2021). Admission to the citizenship of the Republic of Uzbekistan in a simplified manner basics and conditions. ACADEMICIA: An International Multidisciplinary Research Journal, 11(3), 1421-1424.
9. Brenner S.W. Cybercrime: Criminal Threats from Cyberspace. – Santa Barbara: Praeger, 2010. – 281 p.
10. Gercke M. Understanding Cybercrime: Phenomena, Challenges and Legal Response. – Geneva: International Telecommunication Union (ITU), 2014. – 366 p.
11. Ismoilov I., Ziyodullayev M.Z. Ichki ishlar organlarining huquqbuzarliklar profilaktikasi faoliyati: Darslik. – Toshkent: O‘zbekiston Respublikasi IIV Akademiyasi, 2021. – 412 b.

12. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed. – London: Academic Press, 2011. – 840 p.
13. O‘zbekiston Respublikasining «Axborotlashtirish to‘g‘risida»gi Qonuni. 560-II-son. 11.12.2003-y. // O‘zbekiston Respublikasi Oliy Majlisining Axborotnomasi. – 2004. – № 1-2. – 10-m.
14. Юлдашев, Д. Х. (2025). ИЧКИ ИШЛАР ОРГАНЛАРИ ХОДИМИНИНГ ИМИЖИНИ ЯХШИЛАШГА ДОИР ЗАМОНАВИЙ ЁНДАШУВЛАР. Central Asian Journal of Education and Innovation, 4(8), 93-97.
15. Abdurasulova Q.R. Kriminologiya: Darslik. – Toshkent: TDYU nashriyoti, 2018. – 344 b.