KIBERJINOYATLAR VA ULARNING HUQUQIY JIHATLARI

Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti
Imamaliyev Aybek Turapbayevich
"Kriptologiya" kafedrasi Ph.D. dotsent
Hafizov Shukrullo, Xamidov Abdulloh, Rajabov Xurshid, Rabbimov Javlon
Kiberxavfsizlik fakulteti talabalari

Annotatsiya:*Mazkur maqolada Xalqaro va milliy qonunchilik doirasida kiberjinoyatlar va ularga qarshi chora-tadbirlar tahlil qilingan. Kiberjinoyatlar tobora ortib borayotgan zamonaviy davrda ularning oldini olish uchun huquqiy asoslarni mustahkamlash va takomillashtirish zarur. Maqola ushbu sohadagi xalqaro va milliy tajribalarni tahlil qilib, kiberjinoyatchilikka qarshi samarali kurashish yo'llarini o'rganadi.*

Kalit so'zlar: *Kiberjinoyatchilik, huquqiy asoslar, kiberxavfsizlik, xalqaro hamkorlik, jinoyatchilik profilaktikasi, axborot texnologiyalari, qonunchilik.*

Kirish

So'nggi yillarda axborot texnologiyalari rivojlanishi bilan birga kiberjinoyatchilik ham ortib bormoqda. Bu turdagi jinoyatlar nafaqat iqtisodiy zarar yetkazadi, balki shaxsiy ma'lumotlarning o'g'irlanishi, davlat xavfsizligi va ijtimoiy tinchlikka tahdid soladi. Shuning uchun kiberjinoyatchilikka qarshi kurash muhim va zamonaviy vazifa bo'lib, uni amalga oshirishda huquqiy asoslarni mustahkamlash zarur.

Kiberjinoyatchilikka qarshi kurashni kuchaytirish uchun huquqiy asoslarni mustahkamlash va xalqaro hamkorlikni kengaytirish muhim ahamiyat kasb etadi. Mamlakatlar zamonaviy texnologiyalarga asoslangan jinoyatlarni aniqlash va oldini olishda qo'llaniladigan yondashuvlarni takomillashtirishlari zarur. Shu bilan birga, qonunchilik tizimini doimiy ravishda rivojlantirib borish kiberjinoyatchilikning oldini olishga xizmat qiladi.

Metodologiya

Tadqiqotda huquqiy-normativ hujjatlar tahlili, xalqaro tajriba o'rganilishi va qiyosiy huquqiy tahlil usullari qo'llanildi. Kiberjinoyatchilikning oldini olishga qaratilgan qonunchilik me'yorlari, milliy va xalqaro darajadagi yondashuvlar ko'rib chiqildi.

Kiberjinoyatchilikka qarshi kurash borasida eng rivojlangan davlatlar – AQSh, Buyuk Britaniya, Germaniya, Janubiy Koreya, Yaponiya kabi mamlakatlar qator innovatsion yondashuv va kuchli huquqiy tizimni joriy etgan. Quyida ushbu davlatlarning asosiy tajribalari va yondashuvlari keltirilgan:

1. AQSH. AQShda kiberjinoyatchilikka qarshi kurash davlat va xususiy sektor o‘rtasidagi keng hamkorlik asosida amalga oshiriladi. Ushbu mamlakatda Cybersecurity and Infrastructure Security Agency (CISA) kabi tashkilotlar mavjud bo‘lib, ular mamlakatning barcha muhim axborot infratuzilmalarini himoya qilishga qaratilgan. Bundan tashqari, AQSh qonunchiligida Computer Fraud and Abuse Act (CFAA) kabi kiberjinoyatchilikka oid qoidalar mavjud bo‘lib, bu qonun kompyuter tarmoqlariga ruxsatsiz kirishni jinoyat sifatida belgilaydi. Shu bilan birga, kiberjinoyatlarni tez aniqlash va ularning oldini olishda sun’iy intellekt texnologiyalari keng qo‘llanilmoqda.

2. Buyuk Britaniya. Buyuk Britaniyada National Cyber Security Centre (NCSC) tomonidan kiberjinoyatchilikka qarshi chora-tadbirlar amalga oshiriladi. NCSC davlat, tijorat tashkilotlari va jamoatchilik o‘rtasida axborot xavfsizligini ta’minlash bo‘yicha muhim rol o‘ynaydi. Buyuk Britaniya hukumati ushbu sohada doimiy ravishda xalqaro hamkorlikni kuchaytirib, davlatlararo ma’lumot almashinuvini amalga oshiradi. Computer Misuse Act qonuni kiberjinoyatchilikni tartibga soladi va jinoiy javobgarlikni belgilaydi.

3. Germaniya. Germaniyada kiberjinoyatchilikka qarshi kurashda Federal Office for Information Security (BSI) faoliyat ko‘rsatadi. Ushbu tashkilot mamlakatning muhim infratuzilmalarini kiber tahdidlardan himoya qilish va xususiy sektor bilan yaqin hamkorlikni amalga oshirishga mas'uldir. Shuningdek, Germaniyada axborot xavfsizligi bo‘yicha xalqaro hamkorlik kuchli rivojlangan, Yevropa Ittifoqining ENISA (European Union Agency for Cybersecurity) agentligi bilan muntazam hamkorlik qilinadi.

4. Janubiy Koreya. Janubiy Koreyada kiberjinoyatchilikka qarshi kurashda texnologiyalar va IT- kompaniyalarning resurslaridan keng foydalaniladi. Hukumat Korean Internet & Security Agency (KISA) orqali axborot xavfsizligini ta’minlaydi va kiberjinoyatlarni aniqlash hamda ularni oldini olish uchun katta e’tibor qaratadi. KISA mamlakatda internet xavfsizligi to‘g‘risidagi qonunchilikni ishlab chiqishda va tadbirlarni muvofiqlashtirishda muhim rol o‘ynaydi.

5. Yaponiya. Yaponiyada kiberjinoyatchilikka qarshi kurashda National Center of Incident Readiness and Strategy for Cybersecurity (NISC) faoliyat ko‘rsatadi. Ushbu tashkilot davlat va tijorat sektori uchun axborot xavfsizligini ta’minlashda muhim ahamiyat kasb etadi. Yaponiyada kiberjinoyatchilikka qarshi kurashda IT va AI texnologiyalari yordamida kiber tahdidlarni prognozlash va ularni oldini olish usullari ishlab chiqilgan.

Natijalar

Tahlil natijalari shuni ko‘rsatdiki, kiberjinoyatchilikka qarshi kurashning samaradorligi bevosita huquqiy asoslarning mustahkamligiga bog‘liq. Ko‘plab davlatlar kiberjinoyatlarni jinoyat kodeksiga kiritgan bo‘lsa-da, ularga qarshi kurashda xalqaro hamkorlikning kuchaytirilishi lozim. Shu bilan birga, kiberjinoyatlarning yangi turlari paydo bo‘layotgani sababli mavjud qonunchilik doimiy yangilanishni talab etmoqda.

Eng rivojlangan davlatlar tajribasi kiberjinoyatchilikka qarshi kurashni samarali olib borish uchun quyidagilarni tavsiya etadi:

Kuchli huquqiy asoslar va kiberxavfsizlik bo‘yicha maxsus qonunlar joriy etish; Davlat va xususiy sektor o‘rtasidagi yaqin hamkorlik;

Sun’iy intellekt va boshqa yangi texnologiyalardan keng foydalanish;

Xalqaro hamkorlik va axborot almashinuvi orqali tajriba va resurslarni birlashtirish; Axborot xavfsizligi markazlarini tashkil etish va ularni doimiy ravishda rivojlantirib borish.

Bu yondashuvlar O‘zbekistonda kiberjinoyatchilikka qarshi kurashda foydalanilishi mumkin bo‘lgan samarali model sifatida ko‘rib chiqilishi mumkin.

O‘zbekistonga olib kirilishi mumkin bo‘lgan kiberjinoyatchilikka qarshi kurash yo‘nalishlari quyidagi asosiy sohalarni o‘z ichiga oladi. Bu yondashuvlar xalqaro tajriba va kiberxavfsizlikni rivojlantirish borasidagi zamonaviy ehtiyojlar asosida tanlangan.

1. ***Huquqiy Asoslarni Takomillashtirish.*** **Kiberjinoyatchilikka qarshi samarali kurash uchun O‘zbekistonda huquqiy tizimni kuchaytirish zarur:**

Maxsus kiberjinoyatlar to‘g‘risidagi qonunlar: Eng rivojlangan davlatlarda mavjud bo‘lgan Computer Fraud and Abuse Act kabi qonunchilik asoslarini yaratish. Bu qonunlar kiberjinoyatlarning turli shakllarini, jumladan, ruxsatsiz kirish, ma’lumotlarni o‘g‘irlash, zarar yetkazish kabi holatlarni qamrab oladi.

Jinoiy javobgarlik tizimini kengaytirish: Yangi turdagi kiberjinoyatlarni qonuniy tartibga solish va jinoyatchilarni aniqlashda jazo choralarini kuchaytirish.

2. ***Maxsus kiberxavfsizlik markazlarini tashkil etish.*** **O‘zbekiston sharoitida kiberjinoyatchilikka qarshi kurashish uchun davlat va xususiy sektor bilan ishlaydigan kiberxavfsizlik markazlarini tashkil etish quyidagi yo‘nalishlarda samaradorlikni oshiradi:**

Davlat Kiberxavfsizlik Markazi: AQShning CISA yoki Buyuk Britaniyaning NCSC tajribasidan foydalangan holda, barcha davlat organlari va muhim infratuzilmalarni nazorat qiluvchi kiberxavfsizlik markazini yaratish.

Favqulodda vaziyatlarda choralar ko‘ruvchi maxsus guruh: Xavfsizlik hodisalariga tezkor javob beruvchi IT mutaxassislarini tayyorlash.

3. ***Davlat va xususiy sektor hamkorligi.*** **O‘zbekistonda davlat va xususiy sektor o‘rtasidagi hamkorlikni kuchaytirish orqali kiberxavfsizlikni yanada yaxshilash mumkin:**

Axborot almashinuv tizimlari: Xususiy va davlat sektoridagi tashkilotlar o‘rtasida kiberhujumlar, tahdidlar va yangiliklar haqidagi ma’lumotlarni tezkor almashish tizimini yaratish.

Xavfsizlik standartlari va sertifikatlash: Kompaniyalarga kiberxavfsizlik bo‘yicha yuqori standartlarni joriy etishni talab qiluvchi standartlar va sertifikatlash tizimlarini rivojlantirish.

4. ***Zamonaviy Texnologiyalardan Foydalanish.*** **Kiberjinoyatchilikka qarshi kurashda texnologiyalar katta ahamiyatga ega bo‘lib, quyidagi yo‘nalishlarda foydalanish mumkin:**

Sun’iy intellekt va mashina o‘rganish: Kiberjinoyatlarni aniqlash, prognozlash va tahdidlarni o‘z vaqtida bartaraf etishda sun’iy intellekt texnologiyalaridan foydalanish.

Kiberxavfsizlik uchun blockchain texnologiyalari: Blockchain texnologiyalaridan foydalanish orqali axborot tizimlari xavfsizligini mustahkamlash.

5. ***Xalqaro Hamkorlikni Kuchaytirish.*** **Kiberjinoyatchilik global muammo hisoblanganligi sababli, O‘zbekiston quyidagi sohalarda xalqaro hamkorlikni rivojlantirishi lozim:**

Interpol va xalqaro tashkilotlar bilan hamkorlik: Kiberjinoyatchilarni qidirish va ushlashda Interpol va boshqa xalqaro tashkilotlar bilan o‘zaro ma’lumot almashish.

Kiberxavfsizlik bo‘yicha xalqaro tajriba almashish dasturlari: Xodimlarni xorijiy kiberxavfsizlik agentliklarida o‘qitish va tajriba almashishni tashkil etish.

6. ***Jamiyatda Kiberxavfsizlik Savodxonligini Oshirish.*** **Kiberjinoyatchilikka qarshi samarali kurash uchun aholining bilim va malakasini oshirish zarur:**

Aholi uchun o‘quv dasturlari: Kiberxavfsizlikka oid asosiy tushunchalarni o‘rgatuvchi dasturlarni joriy etish, xususan, o‘qituvchilar va talabalar uchun maxsus kurslarni taklif qilish.

Xodimlar uchun muntazam trening va seminarlar: Korxona va tashkilotlar xodimlari uchun kiberxavfsizlikka oid muntazam trening va seminarlarni o‘tkazish, ularning zararli dasturlardan himoyalanish ko‘nikmalarini oshirish.

7. ***Kiberjinoyatchilikka Qarshi Infratuzilmani Rivojlantirish.*** **Kiberjinoyatchilikka qarshi samarali kurashish uchun texnik infratuzilma va texnologik vositalarni rivojlantirish zarur:**

Yuqori texnologiyali axborot xavfsizligi tizimlari: O‘zbekiston sharoitida muhim infratuzilmalarni himoya qilish uchun xavfsizlik tizimlarini, ayniqsa davlat sektoridagi axborot tizimlarini modernizatsiya qilish**.**

Muhokama

Kiberjinoyatchilikning global muammoga aylanishi bu sohada xalqaro hamkorlik va axborot almashinuvini kuchaytirish zaruratini taqozo etadi. Ayrim davlatlarda bu borada samarali tajriba shakllangan, biroq xalqaro darajada integratsiyalashuv hozircha sust. Shu sababli, har bir davlat o‘z qonunchiligini takomillashtirish va yangi texnologiyalarni tatbiq etish orqali kiberjinoyatchilikka qarshi kurashish choralari ko‘rishi kerak.

Qo`shimcha ma`lumot:

Kiberjinoyatchilikka qarshi kurashning huquqiy jihatlari

1. Kiberjinoyatchilik zamonaviy dunyoda tez rivojlanayotgan muammolardan biri bo‘lib, u davlat, xususiy sektor va jamoatchilik uchun xavfsizlik va axborot sirlarini himoya qilishda katta tahdid tug‘diradi. Kiberjinoyatlar orasida shaxsiy ma’lumotlarni o‘g‘irlash, kompyuter tarmoqlariga ruxsatsiz kirish, xakerlik, firibgarlik va boshqa jinoyatlar keng tarqalgan. Shu sababli, ushbu muammoning huquqiy jihatlarini tahlil qilish va huquqiy asoslarni mustahkamlash muhim vazifa hisoblanadi.

2. ***Kiberjinoyatchilikka qarshi kurashning huquqiy jihatlari***

a) *Huquqiy asoslarni yaratish*

Kiberjinoyatchilik bilan kurashish uchun har bir davlatda mustahkam huquqiy asoslar yaratilishi zarur. Bunda kiberjinoyatlar turli toifalarga bo‘linadi: ruxsatsiz kirish, firibgarlik, axborot tizimlariga zarar yetkazish va ma’lumotlarni o‘g‘irlash.

Jinoyat kodeksi va axborot xavfsizligiga oid maxsus qonunlar kiritilishi kerak.

b) ***Xalqaro hamkorlik***

Kiberjinoyatchilikning global xususiyati sababli, davlatlararo hamkorlik kiberjinoyatlarga qarshi samarali kurash uchun muhimdir. Bu Interpol, Europol va boshqa xalqaro tashkilotlar orqali ma’lumot almashish, jinoyatchilarni izlashda yordam beradi.

Xalqaro konvensiyalar, xususan, Budapesht Kiberjinoyatchilik Konvensiyasi, kiberjinoyatchilikka qarshi kurashda xalqaro qonunchilik asosini yaratadi. O‘zbekiston ushbu konvensiyaga qo‘shilish orqali global hamkorlikni kuchaytirishi mumkin.

c) ***Kiberxavfsizlik agentliklari***

Kiberjinoyatchilikka qarshi kurashda maxsus agentlik va organlarning tashkil etilishi katta ahamiyatga ega. Masalan, AQShda Cybersecurity and Infrastructure Security Agency (CISA), Buyuk Britaniyada National Cyber Security Centre (NCSC) faoliyat ko‘rsatadi.

O‘zbekistonda ham shunga o‘xshash markazlarni tashkil etish orqali davlat va xususiy sektor kiberxavfsizligini ta’minlash samaradorligini oshirish mumkin.

d) ***Davlat va xususiy sektor hamkorligi***

Rivojlangan davlatlarda davlat va xususiy sektor o‘rtasidagi hamkorlik kiberjinoyatlarga qarshi kurashda samaradorlikni oshiradi. O‘zbekistonda davlat organlari va kompaniyalar o‘rtasida axborot xavfsizligini ta’minlash bo‘yicha maxsus kelishuvlar va hamkorlik dasturlarini yo‘lga qo‘yish zarur.

e) ***Axborot xavfsizligi standartlari***

Kompaniyalarga axborot xavfsizligi bo‘yicha xalqaro standartlarga moslashishni talab qilish kerak. ISO/IEC 27001 kabi standartlar xodimlar va infratuzilmani xavfsiz saqlashda muhimdir.

Standartlarni qabul qilish orqali mamlakatda kiberjinoyatchilikka qarshi kurashish uchun kuchli asos yaratiladi.

3. ***Kiberjinoyatchilikning Huquqiy Tasnifi***

Kiberjinoyatlar turli shakllarda namoyon bo‘ladi va ularning huquqiy jihatdan to‘g‘ri tasnifi juda muhim:

Kiberfiribgarlik: Internet orqali moliyaviy firibgarlik qilish, yolg‘on ma’lumotlar tarqatish orqali mablag‘ o‘g‘irlash.

Ruxsatsiz kirish: Axborot tizimlariga ruxsatsiz kirib, maxfiy ma’lumotlarni o‘g‘irlash yoki ularga zarar yetkazish.

Kiberxakerlik: Kompyuter tizimlarini buzish, dasturlarni manipulyatsiya qilish.

Axborot xavfsizligi buzilishlari: Tashkilot yoki jismoniy shaxslarning shaxsiy ma’lumotlariga tajovuz qilish, ularni boshqa maqsadlarda ishlatish.

4. ***O‘zbekiston uchun Tavsiyalar***

a) *Huquqiy me’yorlarni mustahkamlash*

Kiberjinoyatlarga oid milliy qonunchilikni xalqaro standartlarga moslashtirish.

Computer Fraud and Abuse Act kabi maxsus qonunchilik asoslarini ishlab chiqish va kiberjinoyatlar uchun alohida javobgarlik turlarini joriy etish.

b) ***Kiberxavfsizlikka oid maxsus markazlarni tashkil etish***

Davlat sektoridagi kiberjinoyatchilikka qarshi chora-tadbirlarni muvofiqlashtiradigan maxsus markaz tashkil qilish.

c) ***Kiberxavfsizlik bo‘yicha xodimlarni tayyorlash***

Mutaxassislar tayyorlash va ularni xorijiy tajribalar bilan tanishtirish orqali kiberjinoyatchilikka qarshi kurash salohiyatini oshirish.

d) ***Xalqaro hamkorlikni rivojlantirish***

Interpol, Europol va Budapesht Konvensiyasiga a’zo davlatlar bilan hamkorlik qilish orqali jinoyatchilarni qidirish va oldini olishda tajriba almashish.

Yakuniy xulosa

Kiberjinoyatchilikka qarshi kurashni kuchaytirish va uni samarali yo‘lga qo‘yish uchun huquqiy jihatlarni mustahkamlash, xalqaro hamkorlikni kengaytirish va zamonaviy texnologiyalardan foydalanish zarur. Shu bilan birga, davlat va xususiy sektor o‘rtasida kiberxavfsizlikka oid doimiy hamkorlikni kuchaytirish, maxsus

markazlarni tashkil qilish va aholining kiberxavfsizlik savodxonligini oshirish kiberjinoyatchilikka qarshi kurashda ijobiy natijalar beradi.

FOYDALANILGAN ADABIYOTLAR:

1. United Nations Office on Drugs and Crime (UNODC). Comprehensive Study on Cybercrime. United Nations, 2013.
2. Budapest Convention on Cybercrime. Council of Europe, 2001.
3. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity. NIST, 2018.
4. Singer, P. W., & Friedman, A. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2014.
5. International Telecommunication Union (ITU). Global Cybersecurity Index (GCI). ITU, 2020.
6. Clough, J. Principles of Cybercrime. Cambridge University Press, 2010.
7. Europol. Internet Organised Crime Threat Assessment (IOCTA). Europol, 2022.
8. Chertoff, M. Explaining Cybersecurity: The Evolution of the Cyber Threat. Georgetown University Press, 2018.
9. INTERPOL. (2022). Virtual Assets: Trends and Challenges in Cybercrime. INTERPOL Cybercrime Department. URL: https://www.interpol.int