



KIBERJINOYAT: ZAMONAVIY AXBOROT MAKONIDAGI TAHDIDLAR VA ULARNING OLDINI OLISH YO‘LLARI

Termis davlat universiteti Yurisprudensiya Fakulteti talabasi:

Ismatov Saidabrор Muhammad-Ali o'g'li

Ilmiy rahbar: N.Q.Yangiboyev

Annotatsiya: Ushbu maqolada kiberjinoyat tushunchasi, uning asosiy turlari, kelib chiqish sabablari, jamiyat va iqtisodiyotga ta'siri hamda kiberjinoyatlarga qarshi kurashishning samarali usullari yoritilgan. Shuningdek, O'zbekistonda axborot xavfsizligini ta'minlash bo'yicha amalga oshirilayotgan islohotlar va xalqaro tajriba tahlil qilingan.

Kalit so'zlar: kiberjinoyat, axborot xavfsizligi, internet, xakerlik, fishing, zararli dasturlar, shaxsiy ma'lumotlar, kibermakon.

Raqamli texnologiyalarning jadal rivojlanishi inson hayotining barcha sohalarini qamrab oldi. Internet, elektron tijorat, onlayn bank xizmatlari va sun'iy intellektdan keng foydalanish bilan bir qatorda kiberjinoyatlar soni ham ortib bormoqda. Bugungi kunda kiberjinoyatlar nafaqat alohida shaxslar, balki davlatlar, moliyaviy institutlar va yirik kompaniyalar uchun ham jiddiy xavf tug'dirmoqda. Shu sababli axborot xavfsizligini ta'minlash va kiberjinoyatlarga qarshi kurashish dolzarb masalalardan biri hisoblanadi. Kiberjinoyat (cybercrime) – bu kompyuter texnologiyalari, axborot tizimlari, internet tarmoqlari va boshqa elektron vositalardan foydalanish orqali sodir etiladigan noqonuniy xatti-harakatlar majmuasidir. Zamonaviy axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida kiberjinoyatlar soni ham yildan-yilga ortib bormoqda. Bugungi kunda deyarli barcha davlatlar



iqtisodiyoti, bank-moliya tizimi, ta'lim, sog'liqni saqlash va davlat boshqaruvi raqamli texnologiyalarga tayanmoqda. Shu sababli ushbu tizimlarga qarshi qaratilgan har qanday noqonuniy harakat nafaqat alohida shaxs, balki butun jamiyat va davlat xavfsizligiga jiddiy tahdid tug'diradi.

Kiberjinoyatlar turli maqsadlarda sodir etiladi. Ayrim jinoyatchilar moddiy manfaat ko'rishni ko'zlasa, boshqalari maxfiy ma'lumotlarni qo'lga kiritish, tashkilotlar faoliyatini izdan chiqarish yoki siyosiy va mafkuraviy maqsadlarni amalga oshirishni maqsad qiladi. Raqamli texnologiyalar rivojlangan sari kiberjinoyatchilar ham yangi usul va vositalardan foydalanib, murakkabroq hujumlarni amalga oshirmoqda. Shu bois kiberxavfsizlikni ta'minlash bugungi kunning eng dolzarb vazifalaridan biri hisoblanadi.

Kiberjinoyatlar sodir etilish usuli va maqsadiga qarab bir necha turlarga ajratiladi. Eng keng tarqalgan turlaridan biri xakerlik bo'lib, bunda jinoyatchilar kompyuter tizimlari yoki tarmoqlariga ruxsatsiz kirib, ma'lumotlarni o'zgartirish, yo'q qilish yoki o'g'irlashga harakat qiladi. Bunday hujumlar ko'pincha davlat idoralari, banklar va yirik korxonalarga qaratiladi.

Yana bir keng tarqalgan usul fishing (phishing) hisoblanadi. Unda jinoyatchilar soxta elektron xatlar, SMS-xabarlar yoki internet sahifalari orqali foydalanuvchilarni aldab, ularning bank karta ma'lumotlari, login va parollari kabi shaxsiy ma'lumotlarini qo'lga kiritadi. Bugungi kunda fishing hujumlari sun'iy intellekt texnologiyalaridan foydalangan holda yanada ishonchli ko'rinishda amalga oshirilmogda. Shuningdek, zararli dasturlar (malware) yordamida ham ko'plab jinoyatlar sodir etiladi. Malware tarkibiga viruslar, troyan dasturlari, qurtlar (worms), spyware va ransomware kabi dasturlar kiradi. Ayniqsa, ransomware dasturlari foydalanuvchi ma'lumotlarini shifrlab qo'yadi va ularni qayta tiklash evaziga pul talab qiladi.

Bundan tashqari, shaxsiy ma'lumotlarni o'g'irlash, internet firibgarligi, ijtimoiy tarmoqlardagi akkauntlarni buzish, elektron to'lov tizimlariga noqonuniy



aralashish va kibertovlamachilik ham bugungi kunda eng ko‘p uchraydigan kiberjinoyatlar qatoriga kiradi. Kiberjinoyatlarning yuzaga kelishiga turli omillar sabab bo‘ladi. Eng avvalo, foydalanuvchilarning axborot xavfsizligi bo‘yicha bilim va ko‘nikmalari yetarli emasligi jinoyatchilar uchun qulay imkoniyat yaratadi. Ko‘pchilik oddiy va oson topiladigan parollardan foydalanadi yoki shaxsiy ma’lumotlarini begona shaxslarga ishonib topshiradi. Ikkinchi muhim sabab – axborot tizimlarining texnik jihatdan yetarlicha himoyalanganligidir. Dasturiy ta’minotlarni o‘z vaqtida yangilamaslik, litsenziyasiz dasturlardan foydalanish va zamonaviy himoya vositalarining yo‘qligi tizimlarda zaifliklarni yuzaga keltiradi. Bundan tashqari, internet foydalanuvchilari sonining keskin ortishi, elektron tijorat va onlayn bank xizmatlarining rivojlanishi ham kiberjinoyatchilar uchun yangi imkoniyatlarni yaratmoqda. Moddiy manfaat olish istagi, anonimlik imkoniyati va ayrim hollarda jazodan qochish ehtimoli ham kiberjinoyatlarning ko‘payishiga sabab bo‘lmoqda.

Kiberjinoyatlar shaxslar, tashkilotlar va davlat uchun katta iqtisodiy hamda ijtimoiy zarar keltiradi. Avvalo, moliyaviy yo‘qotishlar yuzaga keladi. Bank hisobvaraqlaridan mablag‘larning noqonuniy yechib olinishi, korxonalarning ish faoliyati to‘xtab qolishi yoki muhim ma’lumotlarning yo‘qolishi katta iqtisodiy zarar yetkazadi. Shuningdek, shaxsiy ma’lumotlarning oshkor bo‘lishi fuqarolarning shaxsiy hayot daxlsizligini buzadi. Bu esa identifikatsiya ma’lumotlaridan noqonuniy foydalanish, firibgarlik va boshqa jinoyatlarning sodir etilishiga olib kelishi mumkin.

Davlat miqyosida esa kiberjinoyatlar milliy xavfsizlikka tahdid tug‘diradi. Muhim infratuzilmalar, energetika tizimlari, transport va aloqa tarmoqlariga uyushtirilgan kiberhujumlar mamlakat iqtisodiyoti va xavfsizligiga salbiy ta’sir ko‘rsatishi mumkin. Bundan tashqari, bunday jinoyatlar aholining elektron xizmatlarga bo‘lgan ishonchini kamaytiradi va raqamli iqtisodiyot rivojlanishini sekinlashtiradi.



Kiberjinoyatlarga qarshi samarali kurashish uchun texnik, huquqiy va tashkiliy choralarni birgalikda qo‘llash zarur. Avvalo, foydalanuvchilar murakkab va noyob parollardan foydalanishi, ikki bosqichli autentifikatsiyani yoqishi hamda shaxsiy ma’lumotlarini begona shaxslarga bermasligi kerak. Kompyuter va mobil qurilmalarda litsenziyalangan antivirus dasturlaridan foydalanish, operatsion tizim hamda dasturlarni muntazam yangilab borish xavfsizlikni sezilarli darajada oshiradi. Elektron pochta yoki messenjerlarda kelgan shubhali havolalar va noma’lum fayllarni ochmaslik ham muhim profilaktik choralardan biridir.

Davlat darajasida esa kiberxavfsizlikka oid qonunchilikni takomillashtirish, maxsus vakolatli organlar faoliyatini rivojlantirish, xalqaro hamkorlikni kengaytirish hamda aholi va mutaxassislarning raqamli savodxonligini oshirish muhim ahamiyat kasb etadi. Ta’lim muassasalarida kiberxavfsizlik bo’yicha maxsus fanlarni joriy etish va muntazam targ‘ibot ishlarini olib borish ham kiberjinoyatlar sonini kamaytirishga xizmat qiladi.

Natijada, zamonaviy axborot jamiyatida kiberjinoyatlarga qarshi kurash faqat texnik vositalar bilan emas, balki foydalanuvchilarning huquqiy va axborot madaniyatini yuksaltirish orqali ham samarali amalga oshiriladi. Kompleks yondashuvgina raqamli makonda xavfsizlikni ta’minlash va kiberjinoyatlar xavfini kamaytirishga imkon beradi.

Kiberjinoyatlar zamonaviy jamiyatning eng dolzarb muammolaridan biridir. Raqamli texnologiyalar rivojlanishi bilan birga kiberxavfsizlikni ta’minlash har bir fuqaro, tashkilot va davlatning ustuvor vazifasiga aylanmoqda. Axborot xavfsizligi qoidalariga rioya qilish, zamonaviy himoya vositalaridan foydalanish hamda aholining kiberxavfsizlik madaniyatini oshirish orqali kiberjinoyatlar xavfini sezilarli darajada kamaytirish mumkin.



FOYDALANILGAN ADABIYOTLAR:

1. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida” Qonuni.
2. O‘zbekiston Respublikasi Jinoyat kodeksi.
3. <https://qalampir.uz/uz/news/iiv-0goxlantiradi-internetda-firibgarlikning-noodatiy->
4. <https://iiv.uz/news/kiberjinoyatchilikka-qarshi-kiberxavfsizlik>