RAQAMLI SOYALAR ORTIDAGI TAHDIDLAR: ZAMONAVIY DUNYODA KIBERJINOYATLAR EVOLYUTSIYASI

SHERNAZAROV ELBEK ILHOMOVICH
Buxoro viloyati Peshku tumani ichki ishlar bo'limi boshlig'i podpolkovnik

ANNOTATSIYA

Ushbu maqolada raqamli texnologiyalarning jadal rivojlanishi fonida shakllanayotgan va tobora murakkablashayotgan kiberjinoyatlar evolyutsiyasi tahlil qilinadi. Dastlabki xakerlik urinishlaridan tortib, bugungi kunda sun'iy intellekt, ijtimoiy muhandislik va IoT (Internet of Things) qurilmalari orqali amalga oshirilayotgan murakkab hujumlargacha bo'lgan bosqichlar yoritiladi. Shuningdek, maqolada kiberjinoyatlarning global va lokal ko'rinishlari, ularning jamiyat, iqtisodiyot va davlat xavfsizligiga ta'siri muhokama qilinadi. Tahlil davomida ilg'or tahdidlar, ularni aniqlash va oldini olish yo'llari, shuningdek, xalqaro hamkorlikning zaruriyati haqida fikr yuritiladi. Mazkur ish kiberxavfsizlik sohasidagi yangiliklarga qiziqqan o'quvchilar, tadqiqotchilar va mutaxassislar uchun foydali bo'lishi mumkin.

Kalit so'zlar: *kiberjinoyat, raqamli tahdid, sun'iy intellekt, ijtimoiy muhandislik, IoT xavfsizligi, xakerlik, kiberxavfsizlik, kibermuhit, raqamli transformatsiya*

KIRISH

XXI asrda axborot texnologiyalari hayotimizning ajralmas qismiga aylangan bir davrda, insoniyat taraqqiyotining yangi bosqichi — raqamli muhit shakllanmoqda. Internet, sun'iy intellekt, bulutli texnologiyalar va mobil ilovalar kundalik faoliyatni soddalashtirgan bo'lsa-da, shu bilan birga ko'zga ko'rinmas, ammo jiddiy tahdidlar manbai bo'lib ham xizmat qilmoqda. Aynan mana shu raqamli muhit ortida yashiringan, jamiyat xavfsizligi va shaxsiy erkinlikka tahdid soluvchi holatlardan biri — bu kiberjinoyatlardir.

Dastlab oddiy xakerlik harakatlari sifatida boshlangan bu jarayon, bugungi kunda sun'iy intellektdan foydalangan holda amalga oshirilayotgan, moliyaviy, siyosiy, ijtimoiy sohalarga ta'sir ko'rsatadigan murakkab hujumlarga aylandi.

Kiberjinoyatchilik endilikda nafaqat jismoniy shaxslar, balki yirik korporatsiyalar va hatto butun davlatlar uchun ham dolzarb muammo sifatida ko'rilmoqda.

Ushbu maqolada kiberjinoyatlarning tarixiy shakllanishi, ularning zamonaviy ko'rinishlari va evolyutsiyasi, shuningdek, ularga qarshi kurashish mexanizmlari hamda xalqaro hamkorlikning o'rni atroflicha yoritiladi.

ASOSIY QISM

Kiberjinoyatlar evolyutsiyasi, aslida, insoniyatning texnologik taraqqiyoti bilan birga o‘sib borgan yashirin tahdidlar tarixidir. Dastlab oddiy elektron pochta orqali firibgarlik qilish yoki parollarni buzish kabi primitiv harakatlar bilan boshlangan bu jinoyatlar bugungi kunda sun’iy intellekt, mashinali o‘rganish va raqamli aniqlikdan foydalanuvchi murakkab hujumlarga aylangan. Raqamli dunyo — bu nafaqat imkoniyatlar makoni, balki xavflar, yolg‘onlar va manipulyatsiyalar makoni hamdir.

Kiberjinoyatlar bugungi kunda virtual haqiqat bilan real hayot o‘rtasidagi chiziqni yo‘q qilmoqda. Misol uchun, birgina ijtimoiy tarmoqlarda yolg‘on shaxs yaratish orqali odamlarning shaxsiy ma’lumotlarini qo‘lga kiritish, moliyaviy firibgarliklar amalga oshirish yoki hatto siyosiy qarorlarni manipulyatsiya qilish mumkin bo‘lib qoldi. Bunday holatlarda kiberjinoyatchi ko‘pincha ko‘zga ko‘rinmas bo‘ladi — u "raqamli soyada" yashaydi va tahdid real hayotdagi oqibatlarga olib keladi.

Bugungi dunyoda eng zaif nuqtalardan biri — bu inson omilidir. Hujumlar tobora ko‘proq texnik vositalarga emas, balki inson psixologiyasiga qaratilmoqda. Ijtimoiy muhandislik (social engineering) kabi usullar orqali insonlarning ishonchiga kirib, parollarni yoki maxfiy ma’lumotlarni olish hollari keng tarqalgan. Bu esa kiberxavfsizlikni faqat dasturiy himoya bilan emas, balki axborot madaniyati va ongli yondashuv bilan ham mustahkamlash zarurligini ko‘rsatadi.

Shuningdek, IoT qurilmalari, ya’ni narsalar interneti orqali amalga oshiriladigan hujumlar tobora ko‘paymoqda. Har bir aqlli soat, kameralar, hatto sovitgichlar yoki eshik qulf tizimlari — bularning barchasi potentsial kiberportallar hisoblanadi. Ushbu qurilmalar xavfsizlik darajasi past bo‘lgan tarmoqlarga ulanganida, ular orqali uy tarmog‘iga, shaxsiy fayllarga yoki biznes ma’lumotlarga kirish imkoniyati paydo bo‘ladi.

Amaliy tajriba shuni ko‘rsatmoqdaki, ko‘plab tashkilotlar faqat muammo yuzaga kelgach, kiberxavfsizlik choralarini ko‘rishni boshlaydilar. Bu esa ko‘p hollarda kechikkan qaror bo‘lib, moliyaviy va axborot yo‘qotishlariga olib keladi. Shuning uchun kiberxavfsizlik — bu reaktiv emas, balki proaktiv, ya’ni oldini olishga yo‘naltirilgan yondashuv bo‘lishi kerak.

Kiberjinoyatlarga qarshi kurashda xalqaro hamkorlik alohida ahamiyat kasb etadi. Chunki jinoyatlar chegara tanlamaydi, internet esa millat va davlatga bo‘linmaydi. Bir mamlakatdagi xavfsizlik siyosati boshqasining zaif joylari bilan bog‘liq bo‘lishi mumkin. Shu bois xalqaro qonunchilik, birgalikdagi kiberpolitsiya tizimlari va raqamli monitoring mexanizmlari zarur.

Bundan tashqari, ta’lim sohasida kiberxavfsizlik madaniyatini targ‘ib qilish, o‘quv dasturlariga raqamli savodxonlikni kiritish, yosh avlodda xavfsiz internet muhitini yaratish ko‘nikmalarini shakllantirish kiberjinoyatlar profilaktikasining muhim qismidir.

Kiberjinoyatlarga amaliy misollar jadvali

Kiberjinoyat turi	Amaliy holat (real hayotdagi ko‘rinishi)	Amaliy yondashuv / Qarshi choralar
Fishing (soxta sahifalar)	Ijtimoiy tarmoqdan do‘stingiz “qarz so‘rab” yozadi, ammo bu xaker bo‘ladi.	Har doim telefon orqali tasdiqlang; shaxsiy ma’lumotni yozma shaklda bermang.
Zararli ilovalar (malware)	Telefoningizga bepul Wi-Fi topuvchi ilova yuklaysiz – aslida bu ma’lumotlaringizni yig‘adi.	Ilovani faqat rasmiy Play Market yoki App Store orqali yuklang. Sharhlarni va ruxsat so‘rovlarini diqqat bilan o‘qing.
Parollarni buzish	Bitta parolni barcha saytlar uchun ishlatasiz – bitta sayt buzilsa, hammasi xavf ostida qoladi.	Har bir sayt uchun alohida kuchli parol yarating, parollarni saqlash uchun ishonchli managerlardan foydalaning.
Ijtimoiy muhandislik (social engineering)	Kompaniyangizga qo‘ng‘iroq qilib, “texnik xizmat” deb o‘zini tanishtirib, serverga kirish parolini so‘raydi.	Xodimlarni maxfiylik va tasdiqlash protokollari asosida o‘qitish, har qanday so‘rovni tekshirish.
Deepfake videolar	Mashhur shaxs nomidan soxta video tarqaladi va odamlar moliyaviy yordam yuborishadi.	Rasmiy manbalarni tekshirish, shubhali videolarni tahlil qilish uchun faktchek vositalaridan foydalanish.
QR-kod orqali hujum	Restorandagi QR-kod orqali menyu o‘rniga zararli saytga kiriladi.	Faqat rasmiy joylarda joylashtirilgan QR-kodlardan foydalanish; havola ochilayotganda domen nomini tekshirish.
IoT qurilmalar orqali hujum	Aqlli kamera paroli o‘zgartirilmay qoladi – xaker kirib, uyni kuzatadi.	IoT qurilmalarning standart parolini darhol o‘zgartirish va xavfsizlik yangilanishlarini muntazam tekshirish.
Soxta antiviruslar	Kompyuteringizda “virus bor” degan reklama chiqadi, uni bosasiz – zararli dastur o‘rnatiladi.	Kompyuterga faqat rasmiy va litsenziyali antivirus dasturlarini o‘rnatish; reklamalarga ishonmaslik.

Kiberjinoyat turi	Amaliy holat (real hayotdagi ko‘rinishi)	Amaliy yondashuv / Qarshi choralar
Elektron pochta firibgarligi	“Siz lotereyada yutdingiz” degan xat keladi va bank hisob raqamingiz so‘raladi.	Noma’lum manzildan kelgan xatlarga javob bermaslik; hech qachon shaxsiy ma’lumot yubormaslik.
Bulutli tizimdagi ma’lumotlar talon-taroj qilinishi	Foydalanuvchi umumiy faylga tasodifan muhim hujjatlarni yuklaydi – bu fayl internetda ochiq bo‘lib qoladi.	Fayllarni shifrlash, faqat kerakli odamlarga ko‘rsatish huquqini berish, umumiy havolalarni ehtiyotkorlik bilan tarqatish.

Kiberxavfsizlikda kuchli parol yaratish juda muhimdir. Har bir hisob uchun alohida va murakkab parollarni tanlash zarur. Parollar harflar, raqamlar va maxsus belgilar aralashmasidan tashkil topishi kerak. Shu bilan birga, bir xil paroldan bir nechta sayt yoki xizmatlarda foydalanmaslik kerak. Bu usul sizning hisoblaringizni buzilishdan samarali himoya qiladi.

Ikki faktorli autentifikatsiyani yoqish hisobingiz xavfsizligini oshiradi. Bu usul yordamida parolingizni bilgan shaxs ham qo‘shimcha tasdiqlash bosqichidan o‘tmasa, hisobingizga kira olmaydi. Telefoningizga keladigan kod yoki autentifikator ilovalari yordamida qo‘shimcha himoya qatlamini tashkil etish mumkin.

Shubhali havolalarga juda ehtiyotkorlik bilan qarash kerak. Elektron pochta yoki ijtimoiy tarmoqlarda kelgan noma’lum havolalarni bosishdan avval ularning haqiqiyligini tekshirish zarur. Ko‘pincha xakerlar soxta saytlar yaratib, foydalanuvchilarni aldashga harakat qilishadi. Havolaning manziliga e’tibor bering va kerak bo‘lsa, bevosita rasmiy saytga o‘zingiz kirib, ma’lumotlarni tekshiring.

IoT, ya’ni aqlli qurilmalarning xavfsizligini ta’minlash uchun ularning standart parollarini o‘zgartirish kerak. Ko‘pchilik odamlar yangi sotib olingan kameralar, smart televizorlar yoki uy qurilmalaridagi standart parollarni o‘zgartirmaydi. Bu esa xakerlarga kirish imkonini beradi. Shuning uchun darhol murakkab va noyob parol o‘rnatish muhimdir.

Dasturlar va yangilanishlarni faqat rasmiy manbalardan yuklab olish lozim. Internetda ko‘plab zararli dasturlar tarqalmoqda, ular rasmiy do‘konlar yoki ishlab chiqaruvchilar saytiga o‘xshash soxta saytlardan tarqatiladi. Ilovalaringizni faqat Play Market, App Store yoki ishlab chiqaruvchi saytlaridan yuklab oling va tizimingizni doimiy ravishda yangilab turing. Bu yangilanishlar ko‘pincha xavfsizlikni mustahkamlashga xizmat qiladi.

Antivirus dasturini o‘rnatish va uni muntazam yangilab borish muhimdir. Antiviruslar zararli dasturlarni aniqlash va bloklashda yordam beradi. Doimiy

yangilanishlar orqali u yangi tahdidlarga qarshi kurasha oladi. Kompyuter yoki mobil qurilmangizni muntazam tekshirib turing.

Axborot madaniyatini oshirish kerak. O‘zingiz va atrofdagilaringizni kiberxavfsizlik bo‘yicha muntazam o‘qiting. Firibgarlik usullari doimo o‘zgarib turadi, shuning uchun yangiliklardan xabardor bo‘lish juda muhim.

Shubhali fayllarni yuklab olmaslik va ochmaslik kerak. Elektron pochtangizga noma’lum manbalardan kelgan fayllarga juda ehtiyot bilan qarang. Ularni ochishdan oldin antivirus bilan skanerlang. Ko‘pincha zararli dasturlar aynan shu yo‘l bilan tarqaladi.

Muhim ma’lumotlarni shifrlash va zahira nusxalarini yaratish xavfsizlikni oshiradi. Agar sizning ma’lumotlaringiz buzilgan yoki o‘g‘irlangan taqdirda, zahira nusxalar yordamida ularni qayta tiklash mumkin bo‘ladi. Shifrlash esa ma’lumotlarni o‘g‘rilash holatida ularni o‘qilmas qilib qo‘yadi.

XULOSA

Bugungi raqamli asrda kiberxavfsizlik har bir inson va tashkilot uchun eng ustuvor masalaga aylangan. Internet va zamonaviy texnologiyalar hayotimizni yengillashtirayotgan bo‘lsa-da, ular bilan birga yangi tahdidlar va xavf-xatarlar ham yuzaga kelmoqda. Kiberjinoyatlar tobora murakkablashib, raqamli sohada yashirin tahdidlar ko‘paymoqda. Shu sababli, kuchli parollar yaratish, ikki faktorli autentifikatsiyani faollashtirish, qurilmalarni yangilab borish va shubhali manbalardan ehtiyotkorlik bilan foydalanish kabi amaliy choralarga rioya qilish hayotiy zaruratga aylanmoqda.

Aqlli qurilmalar va IoT texnologiyalari ham xavfsizlikni talab qiladi, chunki standart sozlamalardagi zaifliklar xakerlarga kirish imkonini beradi. Shuningdek, axborot madaniyatini oshirish va muntazam o‘qitish orqali foydalanuvchilarni himoya qilish mumkin. Bu esa nafaqat shaxsiy ma’lumotlarni, balki butun jamiyatning raqamli xavfsizligini mustahkamlaydi.

Natijada, kiberxavfsizlik bo‘yicha ongli yondashuv va amaliy chora-tadbirlar hayotimizni raqamli xavflardan himoya qilishda eng samarali yo‘l hisoblanadi. Har bir foydalanuvchi o‘z xavfsizligi uchun mas’uliyatni his qilishi, yangi tahdidlarga tayyor turishi va zamonaviy texnologiyalarni xavfsiz ishlatishi lozim. Shunda raqamli dunyo biz uchun haqiqiy imkoniyatlar makoni bo‘lib qoladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Abdullayev, O. (2021). Kiberxavfsizlik asoslari. Toshkent: «Ilm-Ziyo» nashriyoti.
2. Islomov, S. (2020). Zamonaviy kiberhujumlar va ularning oldini olish usullari. Toshkent: «Fan va Texnologiya» nashriyoti.
3. Qodirov, A. (2019). Axborot xavfsizligi va kiberxavfsizlik. Toshkent: «O‘zbekiston universiteti» nashriyoti.

4. Raximov, D. (2022). Internet va kiberjinoyatlar: xavfsizlik choralarining samaradorligi. Toshkent: «Taraqqiyot» nashriyoti.