RAQAMLI ASRDA KIBERJINOYATCHILIK: FINTECH TAHDIDLARI, PSIXOLOGIK ALDASHLAR VA TA'LIMNING MUHIMLIGI

International school of finance technology and science Instituti Axborot tizimlari va texnologiyalar yunalishi 1-bosqich talabasi ***Mukhtoralieva Nozima***

kamronbekbg@gmail.com

Annotatsiya*: Ushbu maqolada raqamli asrda kiberjinoyatchilikning rivojlanish tendensiyalari, xususan, moliya texnologiyalari (FinTech) sohasidagi xavf-xatarlar va ijtimoiy muhandislik orqali amalga oshirilayotgan psixologik aldash usullari tahlil qilingan. Kiberxavfsizlik zanjiridagi eng zaif halqa — inson omili ekanligi xalqaro tadqiqotlar asosida yoritilib, maktab va oliy ta'lim muassasalarida raqamli savodxonlikni oshirish, maxsus kiberxavfsizlik fanlarini joriy etish hamda professional kadrlarni tayyorlash tizimini takomillashtirish zarurati ilmiy va amaliy jihatdan asoslab berilgan.*

Kalit so‘zlar: *Kiberjinoyatchilik, kiberxavfsizlik, FinTech tahdidlari, ijtimoiy muhandislik, psixologik aldash, inson omili, raqamli savodxonlik, axborot xavfsizligi ta'limi.*

Asosiy qism. Bugungi kunda axborot texnologiyalari shiddat bilan rivojlanib, hayotimizning har bir jabhasiga kirib bormoqda. Ammo texnologik taraqqiyot o'z o'rnida yangi turdagi xavf — kiberjinoyatchilikning ham keng quloch yoyishiga sabab bo'lmoqda. Eng katta muammo shundaki, kiberhujumlar tizimlarning zaifligidan emas, balki ko'pincha foydalanuvchilarning texnologik bilimlari yetishmasligidan osonlik bilan amalga oshmoqda.

Texnologik bilim yetishmasligi — xavfsizlikdagi asosiy bo'shliq

Ilmiy tilda aytganda, axborot xavfsizligi zanjiridagi eng zaif halqa bu — inson omilidir. Dasturchilar qanchalik mukammal va himoyalangan tizimlarni yaratmasin, foydalanuvchining oddiy raqamli xavfsizlik qoidalarini bilmasligi butun tizimni xavf

ostiga qo'yadi. Keng omma orasida raqamli qurilmalarning ishlash tamoyillari, ma'lumotlar maxfiyligi va internetdagi xavf-xatarlar haqidagi tushunchalarning sayozligi kiberjinoyatchilar uchun unumdor zamin yaratmoqda.

FinTech va psixologik aldash (Ijtimoiy muhandislik)

So'nggi yillarda moliyaviy texnologiyalar (FinTech) sohasi, ya'ni mobil ilovalar orqali bank xizmatlari, onlayn to'lovlar va elektron hamyonlar tizimi keskin o'sdi. Bu qulaylik, o'z navbatida, firibgarlarning asosiy nishoniga aylandi. Bugungi kiberjinoyatchilar har doim ham murakkab kompyuter viruslarini yozib o'tirishmaydi. Ular "ijtimoiy muhandislik" (social engineering) deb ataluvchi sof psixologik aldash usullaridan foydalanadilar.

- **Qo'rqitish va shoshiltirish:** Firibgarlar o'zlarini bank xodimi yoki xavfsizlik xizmati vakili sifatida tanishtirib, "Kartangizdan pul yechilmoqda, zudlik bilan SMS kodni ayting" kabi yolg'onlar bilan odamlarni sarosimaga soladi. Inson miyasi stress va qo'rquv holatida mantiqiy fikrlashni yo'qotadi va osonlik bilan manipulyatsiyaga beriladi.
- **Haddan tashqari jozibador takliflar:** Yolg'on sarmoya fondlari yoki yutuqli o'yinlar orqali odamlarning oson boyish istagidan foydalanishadi.

Bu holatlarning barchasi bitta faktni tasdiqlaydi: jinoyatchilar kompyuterni emas, balki inson psixologiyasini "buzib kirishmoqda".

Kiberxavfsizlikka qarshi kurashning eng samarali strategiyasi: Ta'lim tizimlarni himoya qilish qanchalik muhim bo'lmasin, muammoning tub yechimi faqatgina ta'lim tizimini isloh qilish orqali ta'minlanadi. Kiberjinoyatchilikka qarshi uzoq muddatli va mustahkam immunitet yaratish uchun quyidagi qadamlar amalga oshirilishi shart:

1. Ta'lim tizimiga kiberxavfsizlik fanini kiritish Kiberjinoyatchilikka qarshi kurash texnologiyalardan emas, balki odamlarning o'zidan boshlanishi kerak. Buni tasdiqlovchi fakt shuki, IBM korporatsiyasi va Jahon iqtisodiy forumi (WEF) tadqiqotlariga ko'ra, barcha kiberxavfsizlik buzilishlarining qariyb 95 foizi inson xatosi (human error) tufayli sodir bo'ladi. Foydalanuvchilarning ishonuvchanligi, xavfsizlik qoidalariga e'tiborsizligi jinoyatchilar uchun eng katta "ochiq eshik"

hisoblanadi.

Shu sababli, har bir fuqaro kiberxavfsizlikning boshlang'ich bilimlaridan xabardor bo'lishi bugungi kunning hayotiy zaruratidir. O'rta maktablar va universitetlarning o'quv dasturlariga alohida "Raqamli gigiyena va kiberxavfsizlik" fani majburiy tarzda qo'shilishi kerak. Ayniqsa, moliya, texnologiya va ilm-fan yo'nalishidagi xalqaro ta'lim dargohlarida bu fan kelajak mutaxassislarining moliyaviy texnologiyalar (FinTech) xavfsizligini ta'minlashdagi asosiy qalqoni bo'lib xizmat qiladi. O'quvchilar yoshligidan parollarni boshqarish, shaxsiy ma'lumotlarni tarmoqda himoya qilish va firibgarlik sxemalarini tezda tanib olish ko'nikmalariga ega bo'lishlari shart.

2. Amaliy darsliklar va hayotiy misollar (keyslar) yaratish Quruq nazariyadan iborat kitoblar shiddatli raqamli davr talablariga javob bermaydi. Mutaxassislar 2026-yilga kelib global kiberjinoyatdan ko'riladigan yillik zarar bir necha trillion dollarlardan oshishini ta'kidlashmoqda, va buning salmoqli qismi psixologik aldovlarga to'g'ri keladi. Demak, ta'lim amaliyot bilan bevosita bog'lanishi shart. O'quvchi va talabalarga raqamli qurilmalardan to'g'ri va xavfsiz foydalanishni o'rgatuvchi, faqatgina hayotiy misollar (keyslar) bilan boyitilgan yangi avlod darsliklarini joriy etish lozim. Bunday darsliklarda yirik kriptobirjalar (masalan, Binance), elektron hamyonlar yoki mahalliy bank ilovalarida uchrayotgan real firibgarlik ssenariylari tahlil qilinishi kerak. Shuningdek, soxta xabarlarni (fishing) qanday farqlash, ikki bosqichli autentifikatsiya nima uchun muhimligi kabi mavzular interaktiv tarzda, real voqealar xronikasi asosida tushuntirilishi maqsadga muvofiqdir.

3. Professional kadrlar tayyorlashni yangi bosqichga olib chiqish Keng ommani o'qitish bilan bir qatorda, davlat va yirik tashkilotlar xavfsizligini ta'minlaydigan professional kadrlarga bo'lgan ehtiyoj misli ko'rilmagan darajada ortmoqda. Xalqaro axborot tizimlari xavfsizligi sertifikatsiyasi konsorsiumi (ISC2) hisobotlariga ko'ra, butun dunyo bo'ylab kiberxavfsizlik mutaxassislariga bo'lgan ehtiyoj (workforce gap) millionlab o'rinlarni tashkil etmoqda.

Xulosa

Kiberjinoyatchilik — bu faqatgina huquq-tartibot idoralari yoki IT mutaxassislarining muammosi emas. Bu har birimizning kundalik hayotimizga bevosita ta'sir qiluvchi xavfdir. Bugungi kunda yozish va o'qishni bilish qanchalik muhim bo'lsa, raqamli savodxonlik ham shunchalik ahamiyatli. Ta'lim tizimida kiberxavfsizlik madaniyatini shakllantirish orqaligina biz nafaqat o'z shaxsiy ma'lumotlarimiz va mablag'larimizni, balki butun jamiyatimizning raqamli kelajagini ishonchli himoya qila olamiz.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. **World Economic Forum (WEF).** (2022). *The Global Risks Report.* Jahon iqtisodiy forumi nashri. (Inson xatosi va kiberxavfsizlik bo'yicha global tendensiyalar tahlili).

2. **IBM Security.** (2023). *Cost of a Data Breach Report.* IBM korporatsiyasi. (Kiberhujumlarning asosiy sabablari va ijtimoiy muhandislik oqibatlari).

3. **ISC2 (International Information System Security Certification Consortium).** (2023). *Cybersecurity Workforce Study*. (Global miqyosda axborot xavfsizligi mutaxassislariga bo'lgan ehtiyoj va kadrlar yetishmovchiligi tahlili).

4. **Hadnagy, C.** (2018). *Social Engineering: The Science of Human Hacking.* Wiley nashriyoti. (Psixologik aldash usullari va ijtimoiy muhandislik sirlari).

5. **Mitnick, K. D., & Simon, W. L.** (2002). *The Art of Deception: Controlling the Human Element of Security*. Wiley nashriyoti. (Axborot xavfsizligida inson omili va uning ahamiyati).