KOMPYUTER JINOYATLARI VA KIBERXAVFSIZLIK

Kamola Xusanboyeva Nig’matjonovna
Toshkent “Temurbeklar maktabi” Harbiy akademik litseyi
Informatika fani o‘qituvchisi

Annotatsiya: Ushbu maqolada zamonaviy axborot texnologiyalari rivojlanishi bilan birga vujudga kelayotgan kompyuter jinoyatlari va ularga qarshi kurashish muammolari yoritilgan. Kompyuter jinoyatlari tushunchasi, ularning turlari, sodir etilish usullari va global miqyosda xavfsizlik tahdidlari tahlil qilinadi. Shu bilan birga, kiberxavfsizlik tamoyillari, himoya mexanizmlari, xalqaro tajribalar hamda O‘zbekistonda amalga oshirilayotgan chora-tadbirlar o‘rganiladi. Maqolada foydalanuvchilarning axborot xavfsizligini ta’minlash, kiberhujumlarga qarshi immunitetni shakllantirish va raqamli madaniyatni rivojlantirish bo‘yicha tavsiyalar berilgan.

Kalit so‘zlar: kompyuter jinoyatlari, kiberxavfsizlik, axborot xavfsizligi, kiberhujum, raqamli tahdidlar, antivirus, ma’lumotlarni himoyalash, kiberjinoyatchilik, raqamli madaniyat.

Zamonaviy maktablarda kompyuter darslariga kiberxavfsizlik elementlarini kiritish orqali o‘quvchilarga real hayotda qanday xavflar mavjudligini ko‘rsatish mumkin. Masalan, o‘quvchilarga soxta elektron pochta xabarlari yuborilib, ular phishingni qanday aniqlash bo‘yicha o‘z qarorlarini chiqarishadi. Bu orqali ular xatolarni amalda ko‘rib, to‘g‘ri yo‘lni o‘rganishadi.

Oila a’zolari uchun maxsus kiberxavfsizlik kunlarini tashkil etish ham foydalidir. Bu kunlarda ota-onalar va bolalar birgalikda onlayn xavfsizlik haqida suhbatlashishadi, birgalikda parollarni yangilashadi va har bir qurilmada xavfsizlik sozlamalarini ko‘rib chiqishadi. Bu nafaqat bilim, balki oilaviy madaniyat darajasida xavfsizlikni mustahkamlaydi.

Mahalliy hokimiyatlar tomonidan kutubxona va internet kafelarda "xavfsiz internet" burchaklari tashkil qilinadi. Ushbu burchaklarda foydalanuvchilarga kiberxavfsizlik bo‘yicha qisqa ko‘rsatmalar, eslatmalar va amaliy maslahatlar taqdim etiladi. Internetdan foydalanayotganda oddiy foydalanuvchi o‘zini qanday himoyalashi kerakligi haqida tushuncha hosil qiladi.

Kichik biznes egalari uchun interaktiv seminarlar tashkil qilinadi, unda ishtirokchilar o‘zlarining real saytlariga tahdidli hujumlar misolida zaif tomonlarini aniqlaydilar. Bu seminarlar davomida ularga xavfsizlik devorlari, ikki bosqichli autentifikatsiya va boshqa himoya vositalarini qanday joriy etish bo‘yicha amaliy ko‘nikmalar beriladi.

Oliy o‘quv yurtlarida axborot xavfsizligi bo‘yicha talabalarga mo‘ljallangan maxsus laboratoriyalar tashkil etiladi. Bu laboratoriyalarda talabalar real tahdidlar ssenariysi asosida tarmoqni himoya qilish, zararli dasturlarni aniqlash va zararsizlantirishni mashq qilishadi.

Jamoat joylarida, ayniqsa metro, avtovokzal yoki banklarda raqamli xavfsizlikka oid infografik stendlar o‘rnatiladi. Bu orqali oddiy foydalanuvchi mobil telefon yoki bank kartasidan foydalanganda qanday ehtiyot choralarini ko‘rishi kerakligini anglab yetadi.

Barcha amaliy yondashuvlar foydalanuvchini faqat nazariy emas, balki hayotda yuzaga keladigan tahdidlarga qarshi tayyorlaydi. Shuning uchun kiberxavfsizlikni kundalik turmush qismiga aylantirish muhimdir.

Quyida “Kompyuter jinoyatlari va kiberxavfsizlik” mavzusiga mos kreativ amaliy misollar jadval ko‘rinishida taqdim etiladi. Barcha misollar faqat amaliy va real hayotga yaqin tarzda yoritilgan:

Amaliy holat	Kreativ amaliy yechim
Maktab o‘quvchilari kiberhujum haqida faqat nazariy bilimga ega	Maktabda phishing xatlarini tanib olish bo‘yicha interaktiv o‘yin o‘tkazish
Uyda internetdan foydalanadigan bolalar tasodifiy reklama havolalarini bosadi	Ota-onalar bilan birgalikda "xavfsiz internet" kuni tashkil etib, noto‘g‘ri bosish natijalarini amalda ko‘rsatish
Tadbirkor o‘z saytining himoyasizligini bilmaydi	Tadbirkorlar uchun “saytingni sinab ko‘r” nomli ochiq treninglar o‘tkazish
Jamoat joylarida Wi-Fi orqali foydalanuvchi ma’lumotlari o‘g‘irlanadi	Metro va kutubxonalarda “ochiq Wi-Fi xavfi” bo‘yicha infografik va QR-kodli ogohlantiruvchi stendlar joylashtirish
Talabalar kompyuter jinoyatlarini faqat darslikda o‘rganadi	Virtual laboratoriya orqali kiberjinoyatchi izlarini aniqlash bo‘yicha rolli o‘yinlar tashkil etish
Internet foydalanuvchilari kuchli parol tuzishni bilmaydi	“Parolingga baho ber” onlayn simulyatsiyasini ishlab chiqish va ijtimoiy tarmoqlarda ulashish
Ish joylarida parollar bir necha yildan beri o‘zgartirilmagan	Har oyda “Parol yangilash kuni” tashkil etish va jamoaviy rag‘batlantirish tizimini joriy qilish
Kichik korxonalarda xavfsizlik siyosati mavjud emas	Kiberxavfsizlik siyosatini avtomatik yaratadigan interaktiv platforma orqali korxonaga mos siyosat yaratish

Kiberxavfsizlik sohasida eng muhim omillardan biri bu — foydalanuvchilarning ongini shakllantirishdir. Ko‘pchilik texnik himoya vositalariga tayanadi, biroq foydalanuvchi o‘zi ehtiyot bo‘lmasa, eng zamonaviy himoya tizimi ham samarasiz

bo‘ladi. Shu sababli, kiberxavfsizlikni oddiy foydalanuvchilar uchun tushunarli, amaliy, va kundalik hayotga yaqin shaklda tushuntirish zarur.

Masalan, maktab o‘quvchilariga kompyuter xavfsizligi haqida dars o‘qitishda ularga quruq nazariya emas, balki hayotiy vaziyatlar taqdim etilishi kerak. O‘quvchilarga "Do‘stingizdan shubhali havola keldi, nima qilasiz?" degan ssenariy beriladi. Har bir o‘quvchi o‘z fikrini bildiradi, keyin esa real hayotda qanday xavf tug‘ilishi mumkinligi muhokama qilinadi. Bu amaliy yondashuv orqali bolalar bexosdan zararli linkni ochish xavfini anglaydilar.

Tadbirkorlar uchun esa o‘z faoliyatiga mos bo‘lgan xavf-xatarlar asosida interaktiv treninglar tashkil etish mumkin. Ularga “agar saytingizga foydalanuvchilarning ma’lumotlari o‘g‘irlansa, mijozlar ishonchini qanday tiklaysiz?” degan holat beriladi. Bu orqali biznes egalari kiberxavfsizlik nafaqat texnik masala, balki obro‘ va ishonch bilan bog‘liq ekanini anglaydilar.

Oila a’zolarining raqamli savodxonligini oshirish uchun esa har hafta “xavfsiz internet” kuni joriy etilishi mumkin. Bu kunda bolalar ota-onasiga mobil telefon xavfsizligi, xavfsiz parol tuzish, va ijtimoiy tarmoqlarda shaxsiy ma’lumotlarni oshkor qilmaslik haqida tushuntirish beradilar. Bu ikki yoqlama o‘rganishga olib keladi: bolalar mustahkamlaydi, kattalar esa yangilikni o‘rganadilar.

Yana bir samarali usul raqamli jinoyatlar haqidagi qisqa animatsion roliklar yaratish. Masalan, bir multfilmda bola o‘zining fotosuratini notanish odamlarga yuboradi va keyinchalik bu rasm turli soxta akkauntlarda paydo bo‘ladi. Bu orqali tomoshabinlar vizual tarzda muammoni tushunadilar va ehtiyotkorlikni o‘rganadilar.

Kiberxavfsizlik sohasida zamonaviy texnologiyalarni o‘qitishda ham kreativlik muhim. Talabalar yoki yosh mutaxassislar bilan simulyatsiya darslari tashkil etiladi. Ularga soxta veb-sahifalarni aniqlash, tarmoq orqali hujumni bartaraf qilish yoki zararli fayllarni ajratib olish topshiriqlari beriladi. Bu nazariyani emas, real hayotdagi refleks va tezkor qaror chiqarish qobiliyatini rivojlantiradi.

Bundan tashqari, jamoaviy musobaqalar orqali foydalanuvchilarda xavfsizlik muammolariga e’tibor kuchaytiriladi. Masalan, “Eng kuchli parol” tanlovi tashkil etilib, ishtirokchilar o‘z parolini yaratadi va maxsus tizim ularning parolini baholaydi. Bu orqali foydalanuvchilar kuchli parol tuzish sirlarini o‘zlashtiradilar.

Xulosa qilib aytganda, kompyuter jinoyatlari va kiberxavfsizlik masalalarini yoritishda faqat texnik bilimlar yetarli emas. Bu sohani hayotiy misollar, real vaziyatlar, kreativ mashg‘ulotlar, va hissiy tajriba orqali o‘rgatish samaradorlikni oshiradi. Har bir foydalanuvchi o‘zini raqamli muhitda xuddi haqiqiy dunyodagidek ehtiyot qilishni o‘rganishi zarur va bu faqat amaliy yondashuv orqali mumkin.

XULOSA

Zamonaviy raqamli dunyoda kompyuter jinoyatlari va kiberxavfsizlik masalalari nafaqat texnik mutaxassislar, balki har bir foydalanuvchi uchun muhim ahamiyat kasb

etadi. Axborot texnologiyalarining keng qo‘llanilishi bilan birga kiberjinoyatlar ham turli shakllarda rivojlanmoqda. Shuning uchun jamiyatda raqamli madaniyatni shakllantirish, kiberxavfsizlik bo‘yicha savodxonlikni oshirish va har bir foydalanuvchini himoya mexanizmlaridan xabardor qilish dolzarb vazifaga aylangan.

Kiberxavfsizlikni ta’minlash faqat dasturiy ta’minot bilan emas, balki foydalanuvchilarning ongli yondashuvi, doimiy ogohligi va amaliy ko‘nikmalari bilan mustahkamlanadi. Shu ma’noda, interaktiv treninglar, amaliy mashg‘ulotlar, o‘quv simulyatsiyalari va raqamli gigiyena tadbirlari orqali keng jamoatchilikning ishtirokini ta’minlash muhimdir.

Xulosa qilib aytganda, kompyuter jinoyatlariga qarshi kurashda har bir insonning ishtiroki, ongli harakati va xavfsizlikka bo‘lgan shaxsiy munosabati hal qiluvchi rol o‘ynaydi. Bu esa faqat nazariy emas, balki amaliy, ijodiy va samarali yondashuvlar orqali amalga oshirilishi mumkin.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Karimov A. R. – Axborot xavfsizligi asoslari, Toshkent: “Fan va texnologiya” nashriyoti, 2020.
2. Usmonov B. T. – Kompyuter xavfsizligi va axborot himoyasi, Toshkent: “Iqtisodiyot” nashriyoti, 2019.
3. To‘xtayev Sh. Sh. – Raqamli texnologiyalar va kiberxavfsizlik, Toshkent: “Nuroniy” nashriyoti, 2021.
4. Qodirov N. N. – Kiberjinoyatlar va ularning oldini olish usullari, Toshkent: “Yangi asr avlodi”, 2022.
5. O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi – Axborot xavfsizligi bo‘yicha metodik qo‘llanma, Toshkent, 2023.