KIBER-JINOYATCHILIK VA UNGA QARSHI KURASHISH

Durdubayeva Nargiza Muratbayevna
Qoraqalpoq davlat universiteti stajyor o’qituvchisi
Najimov Muratdin
Yuridika fanlari nomzodi, docent

Annotatsiya: Mazkur maqolada internet tarmog’i va axborot texnologiyalari sohasida yuz berayotgan kiberjinoyatlar haqida qisqacha yoritilgan. Shuningdek, ushbu jinoyatlarning turlari, bu turdagi jinoiy vaziyatlarga qarshi kurash tizimini takomillashtirish, xavfsizlik choralarini ko‘rish bo‘yicha qonunchiligimizda samarali olib borilfyotgan islohotlar yoritilgan.

Kalit so’zlar: globallashuv, kiberxavfsizlik, kiberjinoyat, kiberterrorizm, axborot xuruji, informatsion tahdid, kompyuter jinoyatchiligi, elektron jinoyat.

So‘nggi paytlarda ijtimoiy tarmoqlarda saytlarni buzib kirish, virusli dasturlar tarqatish kabi holatlar juda kòp uchramoqda. Kiber jinoyatlar hozirgi globallashuv davrida jiddiy muammolardan biriga aylandi. **Kiber-jinoyatchilik** atamasi kompyuterlar, tarmoqlar yoki internetni qamrab oluvchi jinoiy faoliyatni nazarda tutadi. Kiber-jinoyatning umumiy misollari quyidagilardir:

- dentifikatsiya o'g'irlanishi;
- Phishing;
- Hacking;
- Jinoiy harakatlarga olib keladigan har qanday axmoqlik yoki yolg'onchilik;
- Spyware.

Kiber jinoyatlarga qarshi kurashish uchun IT-kompaniyalar har doim inson omilini hisobga olishlari kerak, chunki hozirgi vaqtda tajovuzkorlar ijtimoiy muhandislik usullaridan faol foydalanadi. Kiberjinoyatlar asosan moliyaviy daromad olish maqsadida amalga oshiriladi. Yangi texnologiyalar zamonida yangicha atamalar bilan ham tanish bo’lishimiz zarur. Ulardan biri “Kiberhujum”. Kiberhujum ko’pincha siyosiy sabablarga ko’ra bo’ladi. Kiberterrorizm esa, vahima yoki qo’rquvni keltirib chiqarish uchun elektron tizimlarni buzishga qaratilgan. Hozirgi kunda eng keng tarqalgan kibertahdidlardan biri zararli dastur - bu kiberjinoyatchi yoki xakerlarning qonuniy foydalanuvchilar kompyuterini buzish yoki shikastlash uchun yaratgan dasturiy ta’minotdir. Ko’pincha nomaqbul elektron pochta ilovasi yoki qonuniy ko’rinishdagi yuklab olish orqali tarqaladigan zararli dasturlar kiberjinoyatchilar tomonidan pul ishlash yoki siyosiy sabablarga ko’ra kiberhujumlarda foydalanilishi mumkin. Hozirgi vaqtda insonlarni kiberhujumlardan himoya qilish maqsadida boshqa

davlatlar qatorida O’zbekiston Respublikasida ham yangi va birqancha samarali qonun hujjatlari ishlab chiqilmoqda. Bulardan Yangi O‘zbekistonning 2022–2026 yillarga mo‘ljallangan Taraqqiyot strategiyasida O’zbekistonda 2023-2026 yillarga mo’ljallangan O‘zbekiston Respublikasining kiberxavfsizlik strategiyasi ishlab chiqilishi nazarda tutilgan. Strategiyaga ko‘ra, axborot maydonidagi kiberhujum va tahdidlarni monitoring qilish tizimi yanada takomillashtiriladi.

▪ Bunda, “UZ” domen zonasi Internet-makonining kiberxavfsizligini ta’minlashning asosiy yo‘nalishlarini hamda elektron hukumat, energetika, raqamli iqtisodiyot tizimlarini va muhim axborot infratuzilmasiga taaluqli boshqa yo‘nalishlarni himoya qilish bo‘yicha kompleks vazifalar belgilanadi. Shuningdek, kiberjinoyatchilik uchun jinoiy javobgarlik qayta ko‘rib chiqilishi ham ko‘zda tutilmoqda. Strategiyaga ko‘ra, axborot maydonidagi kiberhujum va tahdidlarni monitoring qilish tizimi yanada takomillashtiriladi. Bunda:

- kiberxavfsizlikning yagona tarmog‘ining texnik infratuzilmasini kengaytirish;
- “Kibernetikada innovatsiyalar IT-parki” faoliyatini yanada jadallashtirish;
- IT-parkning hududlardagi raqamli texnologiyalar o‘quv markazlari negizida yoshlarni kiberxavfsizlik asoslari bo‘yicha o‘qitilishini ta’minlash, hamda har yili talaba va o‘quvchilar orasida kiberhujumlarni aniqlash bo‘yicha respublika miqyosida konkurslar o’tkazish nazarda tutiladi. Statistik ma’lumotlarga nazar soladigan bo’lsak, 2024 yilga kelib, kiber jinoyatlardan moliyaviy yo'qotishlar deyarli 70% ga etadi. Juniper Research tadqiqotchilarining fikriga ko'ra, zarar har yili o'rtacha 11 foizga oshadi va 2024 yilga kelib 5 trillion dollardan oshadi. O'tgan yili mutaxassislar kiber jinoyatlardan etkazilgan zararni 3 trillion dollarga baholashgan. Har yili kompaniyalar tobora ko'proq raqamli muhitga bog'liq bo'lib, zarar etkazilishi ma'lumotlarning tarqalishi uchun qonun bo`yicha olinadigan jarimalar tufayli ortadi. Jinoyat kodeksining bir qator moddalarida kompyuter texnikasi vositalaridan foydalanib sodir etiladigan jinoyatlar va ularga nisbatan javobgarlik ko‘zda tutilgan.

O`zbekiston Respublikasi Jinoyat kodeksi, 130-modda. Pornografik mahsulotni tayyorlash, olib kirish, tarqatish, reklama qilish, namoyish etish. Pornografik mahsulotni tarqatish, reklama qilish, namoyish etish maqsadida tayyorlash yoki O‘zbekiston Respublikasi hududiga olib kirish, xuddi shuningdek pornografik mahsulotni reklama qilish, namoyish etish, tarqatish, shu jumladan ommaviy axborot vositalarida, telekommunikatsiya tarmoqlarida yoki Internet jahon axborot tarmog‘ida reklama qilish, namoyish etish, tarqatish, shunday harakatlar uchun ma’muriy jazo qo‘llanilganidan keyin sodir etilgan bo‘lsa bazaviy hisoblash miqdorining to‘rt yuz baravaridan olti yuz baravarigacha miqdorda jarima yoki uch yuz oltmish soatgacha majburiy jamoat ishlari yoxud uch yilgacha axloq tuzatish ishlari bilan jazolanadi.

139-modda. Internet jahon axborot tarmog‘ida joylashtirish orqali tuhmat qilish bazaviy hisoblash miqdorining ikki yuz baravaridan to‘rt yuz baravarigacha miqdorda

jarima yoki uch yuz soatdan uch yuz oltmish soatgacha majburiy jamoat ishlari yoxud ikki yildan uch yilgacha axloq tuzatish ishlari yoki bir yilgacha ozodlikni cheklash bilan jazolanadi. Shu bilan birga biz kiberxavfsizlik haqida ham ma’lumotga ega bólishimiz kerak.

Kiberxavfsizlik - bu kompyuterlar, serverlar, mobil qurilmalar, elektron tizimlar, tarmoqlar va ma’lumotlarni zararli hujumlardan himoya qilish amaliyotidir. U axborot texnologiyalari xavfsizligi yoki elektron axborot xavfsizligi sifatida ham tanilgan. Bu atama biznesdan tortib mobil hisoblashgacha bo’lgan turli kontekstlarda qo’llaniladi va bir necha umumiy toifalarga bo’linishi mumkin. Odatda, **kiberxavfsizlik quyidagilarni anglatadi**: shaxslar, *kiberxavfsizlik* ularning shaxsiy ma'lumotlari o'zi va o'zlari shunday vakolatga ega bo'lganlardan boshqa hech kim uchun mavjud emasligini va ularning kompyuterlari to'g'ri ishlashini va zararli dasturlardan xoli ekanligi, kichik biznes egalari ,kiberxavfsizlik kredit karta ma'lumotlari to'g'ri himoyalanganligini va ma'lumotlar xavfsizligi standartlari savdo nuqtalari registrlarida to'g'ri bajarilishini ta'minlashni o'z ichiga olishi mumkin. Shuningdek, onlayn biznes olib boradigan firmalar, *kiberxavfsizlik* o'z ichiga ishonchli serverlar bilan doimiy ishlaydigan serverlarni himoya qilish kiradi. Yani, kiberxavfsizlik bu o'z navbatida ko'plab turli tashkilotlarga tegishli bo'lgan ko'plab virtual serverlarga ega bo'lgan ko'p sonli serverlarni o'z ichiga olgan ko'plab ma'lumot markazlarini himoya qilishni talab qilishi mumkin.

Axborot xavfsizligi saqlashda ham, tranzitda ham ma’lumotlarning yaxlitligi va maxfiyligini himoya qiladi. Operatsion xavfsizlik ma’lumotlar aktivlari bilan ishlash va himoya qilish jarayonlari va qarorlarini o’z ichiga oladi. Foydalanuvchilarning tarmoqqa kirishda ega bo’lgan ruxsatlari va ma’lumotlarning qanday va qayerda saqlanishi yoki baham ko’rilishini belgilovchi protseduralar shu soyabon ostidadir.

Tarmoq xavfsizligi - bu maqsadli hujumchilar yoki opportunistik zararli dasturlardan qat’iy nazar, kompyuter tarmog’ini buzg’unchilardan himoya qilish amaliyotidir.

Favqulodda vaziyatlarni tiklash va biznesning uzluksizligi tashkilotning kiber-xavfsizlik hodisasiga yoki operatsiyalar yoki ma’lumotlarning yo’qolishiga olib keladigan boshqa hodisaga qanday munosabatda bo’lishini belgilaydi. Favqulodda vaziyatlarni tiklash siyosati tashkilotning o’z operatsiyalari va ma’lumotlarini voqeadan oldingi kabi ishlash qobiliyatiga qaytishi uchun qanday tiklashini belgilaydi. Biznesning uzluksizligi - bu ma’lum manbalarsiz ishlashga urinayotganda tashkilot orqaga tushadigan rejadir.

Ilova xavfsizligi dasturiy ta’minot va qurilmalarni tahdidlardan xoli saqlashga qaratilgan. Buzilgan dastur himoya qilish uchun mo’ljallangan ma’lumotlarga kirishni ta’minlashi mumkin. Muvaffaqiyatli xavfsizlik dizayn bosqichida, dastur yoki qurilma ishga tushirilishidan ancha oldin boshlanadi. Shuni takidlab ótish kerak-ki, insoniyatga

yangi imkoniyotlar yaratilishi bilan birga kiber xurujlar tobora ortib, og’irlashib, xavfli tus olib, xususiy va davlat sektorini bir xilda nishonga olmoqda. Bizneslar va kompaniyalarga tegishli tijoriy sirlar va maxfiy axborotlar o’g’irlanmoqda. Universitet va laboratoriyalarga tegishli ixtirolar o’zlashtirib olinmoqda. Fuqarolar shaxsiy ma’lumotlarini boy berib, firibgarlik qurboniga aylanmoqda.

Vaqt o'tishi bilan himoya usullari yaxshilanmoqda. Tahlilchilar kiber jinoyatchilar kelajakda xavfsizlik tizimlarini mustaqil o'rganishga qodir bo'lgan sun'iy intellektdan foydalanishni boshlashlari haqida ogohlantirmoqda. So'nggi yillarda AI texnologiyasi kiber tahdidlardan himoya qilish uchun faol foydalanilmoqda. Kiberxavfsizlik korporativ madaniyatning tobora muhim qismiga aylanib bormoqda, ammo bu tendentsiya kompyuter tizimlari foydalanuvchilari orasida keng tarqalmadi. Internet tarmog‘idagi ayrim ma’lumot va xabarlar buzg‘unchilik, jinoyatchilik harakatlariga undabgina qolmay, balki bunday axborot tarqatish usullaridan turli ekstremistik guruhlar, buzg‘unchi tashkilotlar, kiberterrorizm vakillarihamda ko‘plab firibgarlar foydalanishga harakat qilmoqdalar. Bunday urinishlar o‘z navbatida jinoyatchilikning yangi turlarini “kashf” etishda va jinoyatning globallashuvida katta rol o‘ynab kelmoqda. Ana shunday “kashfiyot”lardan biri — kompyuter jinoyatchiligi qisqa vaqt ichida o‘zining “yuqori cho‘qqisi” ga ko‘tarildi. Yuqorilardagidan xulosa qilib shuni aytish mumkinki, axborot texnologiyalarisohasi jadal rivojlanib borayotgan zamonda u bilan bog‘liq turli tuman muammolar yuzaga kelmoqda. Shunday ekan, internet xavfsizligini ta’minlash va bu kabi jinoyatlarning oldini olish faqatgina davlatning emas, balki internet xizmatidan foydalanayotgan har bir mustaqil shaxsning ham burchi hisoblanmog‘i darkor. Xodimlarni kiberxavfsizlik asoslariga o'rgatish ushbu sohada xarajatlarni yanada samarali rejalashtirishga yordam beradi.

ADABIYOTLAR

1. Sh. M. Mirziyoyev Xalqimizning roziligi faoliyatimizga berilgan eng oliy bahodir. 2-jild. –T. : “O‘zbekiston” 2018.
2. A. U. Anorboyev Kiberjinoyatchilik, unga qarshi kurashish muammolari va kiberxavfsizlikni ta’minlash istiqbollari. Monografiya. –T. : Milliy gvardiya instituti. 2020.
3. S. K. Ganiyev, A. A. Ganiyev, Z. T. Xudoyqulov Kiberxavfsizlik asoslari. O‘quv qo‘llanma. –T. : “Toshkent” 2020.
4. Salayev N.S., Ro`ziyev R.N Kiberjinoyatchilikka qarshi kurashishga oid milliy va xalqaro standartlar. Monografiya ., – T.: TDYU, 2018
5. Нестерович С.А. Проблемы расследования преступлений, которые стоят пред сотрудниками следственных органов.//Вестник науки и образования. №8. 2018.
6. www.lex.uz
7. www.iiv.uz