KIBER JINOYATCHILIKKA QARSHI IMMUNITET HOSIL QILISH MASALALARI

Primov Baxtiyor Olim o'g'li
Toshkent davlat yuridik universiteti "Jinoyat huquqi, kriminologiya va korrupsiyaga qarshi kurashish" kafedrasi o'qituvchisi, yu.f.f.n
E-mail: baxtiyorprimov@inbox.ru
https://doi.org/10.5281/zenodo.11394491

ARTICLE INFO

Qabul qilindi: 20-May 2024 yil
Ma'qullandi: 25- May 2024 yil
Nashr qilindi: 30- May 2024 yil

KEY WORDS

Kiber jinoyat, elektron pochta, Internet-auksion, milliy kiberxavfsizlik, internet, texnologiya, kiber zo'ravonlik, operatsion tizimlar, to'lov protsessor.

ABSTRACT

Mazkur maqolada, ayni vaqtda O'zbekistonda kiberjinoyatlar, hozirgi muammolar va kiberjinoyatlarga qarshi kurashish, kiber jinoyatchilikning turlari, ularning alomatlari, ular aholining qaysi qatlami orasida ko'proq sodir bo'layotgani, ulardan qanday himoyalanish zarurligi, kiber jinoyatchilikka qarshi aholining barcha qatlami orasida huquqiy ong va madaniyatni rivojlantirish, ya'ni fuqarolarga kiber jinoyatchilikning tashqi belgilari va ulardan qanday birlamchi himoyalanish mumkinligi haqida ma'lumotlarni yetkazish orqali imunitet hosil qilish masalalari tahlil qilingan

Kiberjinoyatni butunlay yo'q qilish va to'liq internet xavfsizligini ta'minlash imkoni bo'lmasa-da, korxonalar tizimlar, tarmoqlar va ma'lumotlar xavfsizligini ta'minlashga chuqur mudofaa yondashuvidan foydalangan holda samarali kiberxavfsizlik strategiyasini qo'llab-quvvatlash orqali uning ta'sirini kamaytirishga erishish mumkin. Kiberjinoyat xavfini quyidagi qadamlar bilan kamaytirish mumkin: biznes va xodimlar uchun aniq siyosat va tartiblarni ishlab chiqish; ushbu siyosat va protseduralarni qo'llab-quvvatlash uchun kiberxavfsizlik hodisalariga javob rejalarini yaratish; tizimlar va korporativ ma'lumotlarni himoya qilish bo'yicha amaldagi xavfsizlik choralarini belgilash; ikki faktorli autentifikatsiya (2FA) ilovalari yoki jismoniy xavfsizlik kalitlaridan foydalanish; imkoni bo'lganda, har bir onlayn hisobda 2FA ni faollashtiring; moliyaviy menejer bilan gaplashish orqali pul jo'natish bo'yicha so'rovlarning haqiqiyligini og'zaki tekshirish; kompaniya elektron pochta xabarlariga o'xshash kengaytmali elektron pochta xabarlarini belgilovchi tajovuzlarni aniqlash tizimi (IDS) qoidalarini yaratish; so'rovlar odatiy emasligini aniqlash uchun pul mablag'larini o'tkazish bo'yicha barcha elektron pochta so'rovlarini diqqat bilan ko'rib chiqish; xodimlarni kiberxavfsizlik siyosati va tartib-qoidalari hamda xavfsizlik buzilgan taqdirda nima qilish kerakligi bo'yicha doimiy ravishda o'qitish; veb-saytlar, so'nggi nuqta qurilmalari va tizimlarini barcha dasturiy ta'minot yangilanishlari yoki yamoqlari bilan joriy qilish; ransomware hujumi yoki ma'lumotlar buzilgan taqdirda zararni kamaytirish uchun ma'lumotlar va ma'lumotlarni muntazam ravishda zaxiralash.

Axborot xavfsizligi va kiberjinoyat hujumlariga qarshilik mahalliy qattiq disklar va elektron pochta platformalarini shifrlash, virtual xususiy tarmoq (VPN) va shaxsiy, xavfsiz domen nomlari tizimi (DNS) serveridan foydalanish orqali ham yaratilishi mumkin [1].

Yuqorida ta’kidlab o‘tilganidek, kiberjinoyat hujumlarini kuzatish va boshqarish bilan maxsus shug‘ullanish uchun AQShning turli davlat idoralari tashkil etilgan. FQBning Kiber-divizioni kiberjinoyatchilar, terrorchilar yoki xorijdagi dushmanlar hujumlariga qarshi kurash bo‘yicha yetakchi federal agentlik hisoblanadi. DHS tarkibida Kiberxavfsizlik va infratuzilma xavfsizligi agentligi (CISA) mavjud. Ushbu guruh muhim infratuzilmani himoya qilish uchun xususiy sektor va davlat tashkilotlari o‘rtasida muvofiqlashtiradi. Bundan tashqari, Kiber jinoyatlar markazi (C3) immigratsiya va bojxona organlarining Milliy xavfsizlik tekshiruvlari (HSI) portfeliga kiritilgan mahalliy va xalqaro tergovlarni qo‘llab-quvvatlovchi kompyuterga asoslangan texnik xizmatlarni taqdim etadi. C3 transchegaraviy noqonuniy faoliyatni o‘z ichiga olgan kiberjinoyatlarga qaratilgan. U HSI yurisdiktsiyasi doirasidagi barcha kiberjinoyatlarni topish va yo‘naltirish uchun javobgardir. C3 kiber jinoyatlar bo‘limi (CCU), bolalar ekspluatatsiyasini tergov qilish bo‘limi (CEIU) va kompyuter sud ekspertizasi bo‘limini (CFU) o‘z ichiga oladi. Kiberjinoyatlarga qarshi kurashish uchun tashkil etilgan idoralar bilan bir qatorda turli qonunlar va qonun hujjatlari qabul qilingan. 2015-yilda Birlashgan Millatlar Tashkilotining Narkotiklar va jinoyatchilik bo‘yicha boshqarmasi (UNODC) kiberjinoyatlar bo‘yicha qonunchilik, oldingi xulosalar va sud amaliyoti hamda elektron dalillarni o‘z ichiga olgan markaziy ma’lumotlar bazasi bo‘lgan kiberjinoyatlar omborini chiqardi. Kiberjinoyatlar omborining maqsadi mamlakatlar va hukumatlarga kiberjinoyatchilarni jinoiy javobgarlikka tortish va to‘xtatishga urinishlarida yordam berishdir. Kiberjinoyatchilikka oid qonunchilik keng jamoatchilikka nisbatan qo‘llanilishi mumkin yoki u faqat ayrim turdagi kompaniyalarga taalluqli bo‘lgan sohaga oid bo‘lishi mumkin. Masalan, Gramm-Lich-Bliley qonuni (GLBA) moliyaviy institutlarga e'tibor qaratadi va mijozlar yozuvlarining xavfsizligi va maxfiyligini oshirishi kerak bo‘lgan yozma siyosat va tartiblarni amalga oshirishni tartibga soladi, shu bilan birga shaxsiy ma’lumotlarni tahdidlar va ruxsatsiz kirish va foydalanishdan himoya qiladi. Kiberbulling va onlayn bezorilik kabi maxsus kiberjinoyatlarga qarshi kurashish uchun boshqa qonun hujjatlari ishlab chiqilgan. AQSh shtatlarining yarmidan ko‘pi ushbu jinoyatlar bilan bevosita bog‘liq qonunlarni amalga oshirdi. Misol uchun, Massachusets qonunida ta’kidlanishicha, onlayn bezorilik 1000 dollargacha jarima, ko‘pi bilan ikki yarim yil qamoq yoki har ikkalasi bilan jazolanishi mumkin bo‘lgan jinoyatdir. Tennessi shtatida onlayn ta’qib qilish A toifasidagi qonunbuzarlik hisoblanadi va sudlangan kiberjinoyatchi ko‘pi bilan 11 oy va 29 kunlik qamoq jazosiga, 2500 dollargacha jarimaga tortilishi mumkin.

Ma’lumki, oldini olish har doim davolashdan ko‘ra yaxshiroqdir. Fuqaro internetdan foydalanishda muayyan ehtiyot choralarini ko‘rishi va kiber jinoyatlar uchun ma’lum profilaktika choralariga rioya qilishlari kerak. Xususan, ta’lim orqali ta’sirlarni aniqlash ayollarga ushbu muammolarni hal qilishga yordam beradi. Elektron pochta orqali yoki suhbat paytida shaxsiy ma’lumotlarni begonalarga oshkor qilish hamda internet xavfsizligini kuchaytirish orqali erishish mumkin. Fotosurat hodisalaridan noto‘g‘ri foydalanish sifatida internet orqali begonalarga biron bir fotosurat yuborishdan qochish kerak kundan kun ortib bormoqda.

Veb-sayt egalari trafikni kuzatishlari va saytdagi har qanday qoidabuzarliklarni tekshirishlari kerak. Bu mas’uliyat zimmasida veb-sayt egalari bu borada aniq qaror qabul qilishlari kerak. Blokcheyn texnologiyasidan foydalanish kerak.

Soxta elektron pochta identifikatorini ro‘yxatdan o‘tkazish jinoyat sifatida ko‘rib chiqilishi kerak.Ruxsatsiz kirishdan himoya qilish uchun ovozni aniqlash, filtrlash dasturi va

yoqa identifikatoridan foydalanish kerak. Yuqori texnologiyali jinoyatlar bo‘yicha maxsus kiberjinoyatlarni tergov qilish bo‘limini shakllantirish kerak. Tez odil sudlovni amalga oshirish uchun elektron sud tizimi va videokonferentsiya tizimidan oqilona kengroq foydalanishni tashkil etish kerak. Qonun chiqaruvchi organlar fuqarolar manfaatlarini hisobga olgan holda qat’iy qonun hujjatlarini qabul qilishlari kerak. Kiber jinoyatlar jabrdiydalariga kompensatsion himoya vositalari orqali to‘liq adolat ta’minlanishi lozim. So‘nggi uch o‘n yillikda kompyuter texnologiyalari zamonaviy hayotning mutlaqo hamma joyda mavjud tarkibiy qismiga aylandi. Hayotimizni qo‘llab-quvvatlash va boshqarish uchun texnologiyaga tobora ortib borayotgan bog‘liqlik misli ko‘rilmagan narsalarni yaratdi. Darhaqiqat, jinoyatning aksariyat shakllari hozirda qandaydir tarzda texnologiyani o‘z ichiga oladi, uyali telefonlar va matnli xabarlar yoki texnologiyaning ko‘proq yangi ilovalaridan foydalanish orqali raqamli qurilmalardan tashqarida mumkin bo‘lmagan jinoyatlar kabi. Kiber makon kiber jinoyatchilar uchun begunoh odamlarga zarar etkazish uchun juda ko‘p imkoniyatlarni taqdim etadi. Internet foydalanuvchilari hali ham kiber zo‘ravonlik yoki kiber jinoyatlar haqida darhol xabar berishga tayyor emas. Kiber makon tranzit makondir. Odamlar kiber-makonda yashamasalar ham, u yerda turli amallarni bajarishadi. Bu xususiyat jinoyatchilarga kiber jinoyat sodir etgandan keyin qochish imkoniyatini beradi. Ko‘pchilik veb-saytlar va bloglar tarmoqdagi ayollar va bolalar xavfsizligi uchun xavfsizlik bo‘yicha maslahatlar beradi. Ammo hali ham ayollar ishtirokida ayollarga nisbatan kiber jinoyatlar ortib bormoqda [2]. Ular oson nishon bo‘lgani uchun va ular osongina qurbon bo‘lishlari mumkin, ya’ni nima uchun ayollar asosiy maqsad qilib olinadi. Darhaqiqat, ko‘p suhbatdosh do‘stlari o‘z ayol do‘stlarini “extirosli”, “jozibali” kabi so‘zlar bilan masxara qilishdan zavqlanishadi. Bu kiber odobsizlikning virtual boshlanishidir. Ular asta-sekin ayol do‘stlarini ishonchga va haqiqiy do‘st kabi o‘z muammolarini muhokama qilishni boshlashadi. Agar qabul qiluvchi uzoqlashsa, bunday xabarlarni jo‘natuvchi davom ettirishga ko‘proq rag‘batlantiriladi. Agar jabrlangan ayol o‘sha paytda bu haqda xabar berganida yoki tajovuzkorni ogohlantirganida muammo hal bo‘ladi. Kiber- jinoyatning oldini olish uchun biz tanimagan odamlar bilan suhbatlashmasligimiz kerak. Biz parollarimizni himoya qilishimiz kerak. Shaxsiy materiallarni kompyuterda saqlash bir qancha salbiy oqibatlar keltirib chiqarishi mumkin, chunki ularga xaker kirishi mumkin. Agar biror narsa noto‘g‘ri bo‘lib tuyulsa, darhol huquqni muhofaza qilish organlariga murojaat qilish zarur.

Ayollar internetdan foydalanishda doimo hushyor bo‘lishlari va ularni kirishi mumkin bo‘lgan saytlarni ochmasliklari kerak. Ular o‘zlarini himoya qilish uchun begonalar bilan suhbatlashmasliklari kerak. Hatto bizning hukumatimiz ham NIC-CERT (National Informatika markazi-Kompyuterning favqulodda vaziyatlarga javob berish guruhi) Hindistonda va uyda kiberjinoyatlarga qarshi kurashish uchun vazirlik kiberxavfsizlik tarmog‘ini mustahkamlash uchun Kiberjinoyatlarni muvofiqlashtirish markazini (I4C) tashkil etishni taklif qilmoqda. Foydalanuvchilar undan foydalanish natijasida yuzaga keladigan zaifliklardan xabardor bo‘lishlari va xavflarini kamaytirish uchun choralar ko‘rishlari mumkin. Kompyuter foydalanuvchilari Internetdan foydalanishning bir necha oddiy qoidalariga rioya qilish orqali kiberjinoyat qurboni bo‘lish xavfini kamaytirish choralarini ko‘rishlari mumkin. Birinchidan, foydalanuvchilar foydalanilmayotganda kompyuterlarini o‘chirishni unutmasliklari kerak. Kiber jinoyatchilar ko‘pincha “har doim yoqilgan” kompyuterlarni qidirib, tarmoqlarni skanerlashadi, ular osonlik bilan kirish mumkin va qarovsiz nishonlar deb hisoblaydilar.

Kompyuterlar yoqilgan va internetga ulangan vaqtni minimallashtirish orqali odamlar xakerlik hujumlariga nisbatan zaifligini kamaytirishi mumkin. Keyinchalik, foydalanuvchilar antivirus va xavfsizlik devori dasturlarini o‘rnatishlari va ularga xizmat ko‘rsatishlari kerak. Ushbu ilovalar kompyuterlarning operatsion tizimlarida xavfsizlik xususiyatlarini chetlab o‘tish uchun mo‘ljallangan viruslar va boshqa zararli kompyuter dasturlariga qarshi birinchi himoya chizig‘i bo‘lib xizmat qiladi. Bundan tashqari, operatsion tizim ishlab chiquvchilari muntazam ravishda yangilanishlar yoki "yamalar" chiqaradilar. Kompyuter xavfsizligini oshirish uchun foydalanuvchilar ushbu yangilanishlar mavjud bo‘lishi bilanoq ularni o‘rnatishlari kerak. Kiber jinoyatchilar ko‘pincha zararli dasturlarni elektron pochta xabarlariga biriktirilgan rasm yoki hujjatlar sifatida yashiradilar, shuning uchun foydalanuvchilar hech qachon noma’lum jo‘natuvchilardan elektron pochta qo‘shimchalarini ochmasliklari yoki yuklab olishlari kerak emas. Endi ko‘p odamlar o‘z uylarida simsiz tarmoqlardan foydalanishadi. Simsiz yo‘riqnoma sozlamalarida kuchli shifrlash kiber jinoyatchilarning kompyuterlarda saqlangan ma’lumotlarga kirishi va ulardan foydalanishining oldini oladi. Tarmoq trafigini himoya qilish uchun shifrlashdan foydalanmaydigan himoyalanmagan yoki “ochiq” simsiz tarmoqlar kiber jinoyatchilar uchun juda mashhur nishonlardir. Ushbu simsiz tarmoq trafigini ushlab turish orqali firibgarlar shaxsiy ma’lumotlar, parollar va boshqa ma’lumotlarni tezda to‘plashlari mumkin, keyin ular turli kiber jinoyatlarni sodir etishda foydalanishlari mumkin. Agar sizning uyingizda shifrlanmagan simsiz tarmoq mavjud bo‘lsa, politsiya sizning kompyuterlarga buzib kirganingiz, onlayn firibgarlik qilganingiz yoki kontrabanda tarqatganingizni bilish uchun eshik oldida paydo bo‘lsa, hayron bo‘lmang. Ko‘p odamlar o‘nlab turli veb-saytlarda hisob qaydnomalarini yuritadilar, shuning uchun ular eslab qolish uchun oson parollar yaratadilar. Bu kamdan-kam ishlatiladigan parolni unutish ehtimoli kamroq degani bo‘lsa-da, bu oddiy parollar aqlli kiber jinoyatchilar tomonidan tezda buzilgan. Bundan tashqari, ko‘p odamlar o‘zlarining ijtimoiy tarmoq veb-saytlarida, bank va brokerlik hisoblarida bir xil paroldan foydalanadilar. Kiber firibgarlar ijtimoiy tarmoq veb-saytlari uchun parollarni o‘g‘irlashganda, ular ko‘pincha moliyaviy hisoblarga kirish uchun ulardan foydalanishga harakat qilishadi. Bunday muammolarni oldini olish uchun odamlar o‘zlarining har bir akkaunti uchun noyob va murakkab parollardan foydalanishlari kerak. Ushbu oddiy qoidalar ko‘pchilik Internet foydalanuvchilari uchun asosiy xavfsizlikni ta'minlaydi. Biroq, odamlar kiber jinoyat qurboni bo‘lish xavfini yanada kamaytirish uchun qo‘llashi mumkin bo‘lgan qo‘shimcha ehtiyot choralari mavjud. Ba’zi keng tarqalgan jinoiy sxemalarni tushunish va tan olish odamlarga ularning qurboni bo‘lishdan qochishga yordam beradi. Keng tarqalgan bir sxemada kiber jinoyatchilar fishing elektron pochta xabarlarini yuborishadi. Ushbu elektron pochta xabarlari qonuniy jo‘natuvchilardan ekanligini yolg‘on da'vo qiladi va shubhasiz qabul qiluvchini parollar, kredit karta raqamlari va bank hisobi ma’lumotlari kabi shaxsiy, nozik ma’lumotlarni oshkor qilishga qaratilgan hujjatlarni o‘z ichiga oladi. Ba’zi fishing elektron pochta xabarlarida qurbonlar muntazam foydalanadigan saytlarga o‘xshash soxta veb-saytlarga havolalar mavjud. Jabrlanuvchilarni bank ma’lumotlari yoki boshqa nozik ma’lumotlarni taqdim etish uchun aldagandan so‘ng, jinoyatchilar jabrlanuvchining pullariga kirish va o‘g‘irlash uchun turli xil usullardan foydalanadilar. Internet-auksionda firibgarlik juda keng tarqalgan. Kiber jinoyatchilar Internet auktsion saytlarini to‘ldirishadi va odamlar izlayotgan deyarli har qanday mahsulotni taklif qilishadi. E’lonlar ko‘pincha sotuvchi xaridor bilan bir mamlakatda

joylashgandek ko‘rinadi va jinoyatchi jabrlanuvchiga pulni biznes sherigi, hamkori, kasal qarindoshi, oila a'zosi va boshqalarga yuborishni maslahat beradi. Pul odatda pul o‘tkazmalari orqali o‘tkaziladi, bu esa jabrlanuvchiga ozgina murojaat qiladi. Eng so‘nggi tendentsiya - bankdan bankka pul o‘tkazmalarining ko‘payishi. Eng muhimi, bu pul o‘tkazmalari yirik banklar orqali o‘tadi, lekin keyin boshqa mamlakatlardagi banklarga yo‘naltiriladi. Huddi shunday, sotuvchilar ham vaqti-vaqti bilan qurbonlarni soxta “escrow” tlaridan foydalangan holda to‘lashga yo‘naltiradilar. Ba'zan ular o‘zlarini yanada vijdonli ko‘rsatish uchun qonuniy eskrov veb-saytlarini o‘g‘irlashadi. Mablag‘lar eskrow veb-saytiga o‘tkazilgandan so‘ng, sotuvchi odatda aloqani to‘xtatadi. Yana bir mashhur sxema – qalbaki kassir cheklarini o‘tkazish. Ushbu sxema tovarlarni sotish uchun Internetda tasniflangan reklamalardan foydalanadigan odamlarga mo‘ljallangan. Odatda, manfaatdor tomon sotuvchi bilan bog‘lanadi. Sotuvchiga aytilishicha, xaridorning jabrlanuvchining mamlakatida unga qarzi bor sherigi bor. Shunday qilib, u sherikdan jabrlanuvchiga xaridorga qarz miqdori uchun kassir chekini yuborishini talab qiladi. Kassir chekining miqdori ko‘pincha tovar narxidan minglab dollarga ko‘p bo‘ladi va jabrlanuvchiga ortiqcha miqdor tovarni uning joylashgan joyiga olib borish bilan bog‘liq yuk tashish xarajatlarini to‘lash uchun sarflanishi aytiladi. Jabrlanuvchiga chekni depozitga qo‘yish va pul mablag‘lari o‘z hisobvarag‘iga o‘tkazilgandan so‘ng, ortiqcha mablag‘ni jinoyatchiga yoki yuk tashish agenti sifatida belgilangan boshqa sherikga qaytarishni buyuradi. Kassir chekidan foydalanilganligi sababli, banklar odatda pul mablag‘larini darhol yoki bir yoki ikki kun ushlab turishdan keyin chiqaradilar. Chekning haqiqiyligiga yolg‘on ishonib, sotuvchi ko‘rsatmalarga muvofiq pulni o‘tkazadi. Oxir-oqibat, bank kassir chekining soxta ekanligini aniqlaydi va bu mablag‘larni jabrlanuvchining hisobidan olib tashlaydi.

Ba’zi odamlar beixtiyor kiber jinoyatchilarning sheriklariga aylanishadi. Jinoyatchilar Internetdagi mashhur ish saytlarida uyda ishlash bo‘yicha takliflarni joylashtiradilar. Ushbu ishlar “moliyaviy menejer” yoki “to‘lov protsessor” lavozimlari sifatida e’lon qilinadi. Ushbu lavozimlarni qabul qilgan odamlarga bank hisob raqamlarini ochishlari va ish beruvchilariga hisob raqamlarini taqdim etishlari aytiladi. Ular ushbu hisobvaraqlarga pul o‘tkazmalarini oladilar va bu pullarni yechib olishlari va (albatta, ularning komissiyasi olib tashlangan holda) xorijiy davlatlardagi belgilangan oluvchilarga o‘tkazishlari topshiriladi. Huquqni muhofaza qilish organlariga murojaat qilganda, bu odamlar kiber jinoyatchilar uchun “pul xachiri” rolini o‘ynaganliklarini bilib hayron qolishadi. Bu odamlar pul mablag‘larini uchinchi shaxslar oluvchisi sifatida harakat qilib, noqonuniy daromadlarni bevosita xorijiy mamlakatlardagi kiberjinoyatchilarga o‘tkazishga yordam berishgan. Kiberjinoyatchilar tomonidan tahdid haqiqiy bo‘lsa-da, internet xavfsizligining bir necha asosiy usullaridan foydalanish va keng tarqalgan kiberjinoyat sxemalaridan xabardor bo‘lish orqali shaxslar qurbon bo‘lish xavfini kamaytirishi mumkin. Foydalanuvchilar so‘nggi onlayn firibgarliklardan xabardor bo‘lishlari kerak, ularning aksariyati www.lookstoogoodtobetrue.com da tasvirlangan. Biroq, agar shaxs o‘zini allaqachon kiberjinoyat qurboni bo‘lgan deb hisoblasa, u imkon qadar tezroq tegishli huquqni muhofaza qilish organini xabardor qilishi kerak va dunyoning istalgan nuqtasidan www.ic3.gov, hamkorlik saytida shikoyat qilishi mumkin. Sxemaning tafsilotlari va jinoyatchilarning xususiyatlarini aniqlaydigan o‘z vaqtida va to‘liq ma’lumot berish huquqni muhofaza qilish organlariga samarali tergov strategiyasini ishlab chiqishga yordam beradi. Skot Xantsberri - nazorat bo‘yicha maxsus agent bo‘lib, u yaqinda Vashingtondagi kiber

bo‘limda FQBda ishlagan. FQBning kiber bo‘limi kiber-asoslangan terrorizm, dushmanlik bilan kurashish uchun eng yuqori darajadagi texnologik imkoniyatlar va tergov tajribasini qo‘llashga bag‘ishlangan. Internet orqali amalga oshirilgan xorijiy razvedka operatsiyalari va kiber jinoyatlar. Kiber-divizionning ishi FQBga Qo‘shma Shtatlarga texnologik tahdid solayotgan dushmanlardan bir qadam oldinda turishga imkon beradi. Kiber-bo‘lim ko‘pincha xalqaro va milliy iqtisodiy ta'sirga ega bo‘lgan kiber aloqa bilan barcha huquqbuzarliklarni ko‘rib chiqadi va bir vaqtning o‘zida dastur yo‘nalishlari bo‘ylab FBI ustuvorliklarini qo‘llab-quvvatlaydi, tajovuzkor texnologik tergov yordami zarur bo‘lganda terrorizmga qarshi kurash, razvedka va boshqa jinoiy tergovlarga yordam beradi.

Internetga qo‘ygan har bir ma’lumot hisobingizni buzishning potentsial usulidir. Agar siz bir nechta ijtimoiy media platformalarida o‘z ishtirokingizni saqlab qolishga jiddiy yondashsangiz, parollaringiz kuchli ekanligiga ishonch hosil qiling. Parollarni muntazam ravishda o‘zgartirish ma’lumotlaringizni xakerlardan himoya qilishning ajoyib usuli hisoblanadi. Kuchli parollar yaratish uchun parol menejeri ilovalaridan foydalanishingiz mumkin. Ikki faktorli autentifikatsiya qo‘shimcha xavfsizlik qatlamini qo‘shadi. Har doim ilovaga kirish ruxsatini so‘rang. Har qanday ilovani yuklab olganingizda har qanday veb-saytga tashrif buyurganingizda, sizdan ma’lum miqdordagi ruxsatnomalar so‘raladi. Agar asosiy ruxsatlar so‘ralsa, bu yaxshi. Biroq, galereyangiz va shunga o‘xshash maxfiy ma’lumotlarga kirish uchun ruxsat so‘ralsa, darhol bunday so‘rovlarni rad eting. Bundan tashqari, darhol veb-saytdan chiqing va ilovani darhol o‘chiring. Bepul Wi-Fi har doim qiziqarli. Ammo ko‘pincha bu sizni undan foydalanishga jalb qilish uchun xakerlar tomonidan qo‘yilgan asal tuzog‘idir. Bepul Wi-Fi orqali internetga kirganingizda, xakerlar qurilmangizga osongina kirishi, viruslarni tarqatishi, ma’lumotlarni o‘g‘irlashi va shunga o‘xshash boshqa narsalarni amalga oshirishi mumkin. Nihoyat, har qanday "haqiqat bo‘lish uchun juda yaxshi" xabarlar, qo‘ng‘iroqlar haqida har doim shubhali bo‘ling. Agar sizga shunday qo‘ng‘iroqlar, xabarlar tushsa, har doim tegishli mansabdor shaxslarga xabar bering.

Kibermakondagi muammolardan biri bu yurisdiktsiyani aniqlashdir. Internet global bo‘lganligi sababli, muayyan vaziyatga qaysi qonunlar qo‘llanilishini aniqlash qiyin bo‘lishi mumkin. Kiberhuquq kibermakondagi yurisdiktsiya masalalarini hal qiluvchi qoidalar va qoidalarni o‘z ichiga oladi, Fuqarolik va tijorat masalalari bo‘yicha sud qarorlarini ijro etish va sud qarorlarini ijro etish to‘g‘risidagi Gaaga konventsiyasi.

Kiberhuquq faqat ayrim mamlakatlar bilan chegaralanib qolmaydi. Internet global bo‘lgani uchun kibermakonni tartibga solishda xalqaro huquq ham rol o‘ynaydi. Kiber huquq xalqaro bitimlar va munosabatlarni tartibga soluvchi qoidalar va qoidalarni o‘z ichiga oladi, masalan, Birlashgan Millatlar Tashkilotining Xalqaro shartnomalarda elektron aloqalardan foydalanish to‘g‘risidagi konventsiyasi.

Kiber huquqni nazorat qiluvchi bir qator tartibga soluvchi organlar mavjud. Bularga davlat idoralari, sanoat guruhlari va xalqaro tashkilotlar kiradi. Nazorat qiluvchi organlar kiber qonunchilikni tatbiq etish va ularga rioya etilishini ta’minlashda muhim rol o‘ynaydi

Xavfsiz va xavfsiz raqamli muhitni ta’minlash uchun kiber-qonunni qo‘llash juda muhimdir. Kiber huquqni qo‘llashning bir qancha usullari, jumladan, jinoiy ta'qiblar va fuqarolik da'volari mavjud. Internetning global tabiati va kiberjinoyatchilarni aniqlash va jinoiy javobgarlikka tortish qiyinligi sababli ijro etish qiyin bo‘lishi mumkin, biroq FQBning Kiber bo‘limi va Yevropa Ittifoqining Kiberxavfsizlik agentligi kabi ixtisoslashgan idoralar

huquqni muhofaza qilishni yaxshilash ustida ishlamoqda.

Kiberhuquqga rioya qilish kibermakonda faoliyat yurituvchi korxonalar va jismoniy shaxslar uchun zarurdir. Kiber qonunlarga rioya qilmaslik jarimalar, sud jarayonlari va obro‘sini yo‘qotish kabi huquqiy va moliyaviy oqibatlarga olib kelishi mumkin. Korxonalar va jismoniy shaxslar uchun ma’lumotlarni himoya qilish choralarini qo‘llash, xodimlarni kiberxavfsizlik bo‘yicha ilg‘or tajribalarga o‘rgatish va rivojlanayotgan texnologiyalardan xabardor bo‘lish kabi muvofiqlikni ta’minlash uchun eng so‘nggi qoidalar va qoidalardan xabardor bo‘lish muhim.

Kiberhuquq jismoniy shaxslar uchun ham muhim ahamiyatga ega. Shaxslar internet va tegishli texnologiyalardan foydalanishda o‘z huquq va majburiyatlarini bilishlari kerak. Kiber qonunlarga rioya qilmaslik shaxslar uchun huquqiy va moliyaviy oqibatlarga olib kelishi mumkin, masalan, shaxsiy ma’lumotlarni o‘g‘irlash va kiber ta'qib qilish, ammo kiber qonunlarni tushunish va ularga rioya qilish shaxslarga shaxsiy ma’lumotlarini himoya qilish va maxfiyligini ta’minlashga yordam beradi.

Kiber huquq - bu huquqning murakkab va doimiy rivojlanib boruvchi sohasi. Kibermakonda faoliyat yurituvchi jismoniy shaxslar va korxonalar uchun eng so‘nggi qoidalar va qoidalardan xabardor bo‘lish juda muhimdir. Kiber qonun va uning oqibatlarini tushunib, biz xavfsizroq va xavfsizroq raqamli muhitni yaratish ustida ishlashimiz mumkin, ammo bu maqsadga erishish uchun jismoniy shaxslar, korxonalar, nazorat qiluvchi organlar va huquqni muhofaza qilish organlarining birgalikdagi sa'y-harakatlarini talab qiladi.

Kuzatuv jamiyatining asosiy qonuniy misollaridan biri jamoat joylarida videokuzatuv kameralaridan foydalanishdir. Hukumatlar jamoat tartibi va xavfsizligini saqlashga yordam berishlarini da'vo qilish bilan ularni joylashtirishni oqlaydi. CCTV (josuslik qilish va aloqalarni kuzatish uchun veb-kameralar) kameralaridan foydalanish, agar u ichki qonunlar va xalqaro inson huquqlari qonunlariga muvofiq bo‘lsa, qonuniydir. Buyuk Britaniyada CCTV kameralaridan foydalanish 2013- yilgi kuzatuv kameralari amaliyot kodeksiga muvofiq tartibga solinadi, bu jamoat joylarida kameralarni joylashtirish standartlarini belgilaydi. Xuddi shunday, Qo‘shma Shtatlarda turli shtatlarda CCTV foydalanish bo‘yicha turli xil qoidalar mavjud va muvofiqlik standarti AQSh Konstitutsiyasiga To‘rtinchi Tuzatish bilan belgilanadi. Yana bir huquqiy misol - yuzni tanish texnologiyasidan foydalanish, bu maxfiylikka oid jiddiy muammolarni keltirib chiqaradi. Xitoyda yuzni tanish texnologiyasi odamlarning xaridlar tarixi, ijtimoiy tarmoqlardagi faoliyati va transport yozuvlari kabi kundalik faoliyatini kuzatish uchun keng qo‘llaniladi. Evropa Ittifoqida Ma’lumotlarni himoya qilish bo‘yicha umumiy reglament (GDPR) yuzni aniqlash texnologiyasidan foydalanish bo‘yicha muhim cheklovlarni belgilab qo‘ydi, uni joylashtirish uchun aniq rozilikni talab qiladi va shaxsiy ma’lumotlarning maxfiyligiga bo‘lgan huquqlarini himoya qiladi. Etakchi yurisdiktsiyalar: Kuzatuv jamiyatining etakchi yurisdiktsiyasi Xitoy bo‘lib, u o‘z aholisini kuzatish uchun ilg‘or kuzatuv texnologiyalaridan foydalanadi. Bularga yuzni aniqlash texnologiyasi, ijtimoiy kredit tizimlari va dronlar va boshqalar kiradi. Bunday texnologiyalardan norozilikni bostirish va siyosiy muxolifatni kuzatish uchun foydalanish mumkinligidan xavotirlar bildirilgan, chunki hukumat tomonidan suiiste'mol qilinishining oldini olish uchun huquqiy kafolatlar kam. Aksincha, Evropa Ittifoqi kuzatuv texnologiyalari bo‘yicha qat'iyroq qoidalarga ega, GDPR bunday texnologiyalardan foydalanish bo‘yicha aniq cheklovlarni belgilaydi va alohida mamlakatlar sudlari ushbu standartlarni qo‘llaydi. O‘zbekistonda kuzatuv texnologiyalari

to‘g‘risidagi qonun bir qancha normativ-huquqiy hujjatlar bilan tartibga solinadi, jumladan:

1. O‘zbekiston Respublikasi Konstitutsiyasi – bu fuqarolarning shaxsiy daxlsizligi va yozishmalar, telefon suhbatlari, pochta, telegraf va boshqa xabarlar sir saqlanishini kafolatlaydi.

2. “Axborot texnologiyalari va kommunikatsiyalari to‘g‘risida”gi qonun – bu elektron aloqa vositalaridan foydalanishni tartibga soladi va xizmat ko‘rsatuvchi provayderlarning foydalanuvchilarning shaxsiy hayotini himoya qilish bo‘yicha majburiyatlarini belgilaydi.

3. "Tezkor-qidiruv faoliyati to‘g‘risida"gi qonun - bu huquqni muhofaza qilish organlari tomonidan kuzatuv va boshqa tergov faoliyatini amalga oshirish tartibini belgilaydi.

4. “Davlat siri to‘g‘risida”gi qonun – bu davlat siri hisoblangan ma’lumotlarni maxfiylashtirish va himoya qilishni tartibga soladi, unga kuzatuv texnologiyalari bilan bog‘liq ma’lumotlar kiradi. Ushbu qonunlarga ko‘ra, milliy xavfsizlik, huquqni muhofaza qilish va jinoyatchilikning oldini olish maqsadlarida kuzatuv texnologiyalaridan foydalanishga odatda ruxsat etiladi. Biroq, har qanday kuzatuv faoliyati qonuniy tartib-qoidalar va konstitutsiyaviy shaxsiy hayot va maxfiylik kafolatlariga muvofiq amalga oshirilishi kerak. Kuzatuv texnologiyalari bo‘yicha O‘zbekiston qonunchiligini qanday yaxshilash mumkin?

1. Kuzatuv texnologiyalari doirasini va ulardan foydalanish mumkin bo‘lgan sharoitlarni aniq belgilash.

2. Kuzatuv texnologiyalaridan faqat qonuniy maqsadlarda foydalanilishi va ulardan foydalanish nazorat va javobgarlikka tortilishini ta’minlash.

3. Kuzatuv texnologiyalari orqali olingan ma’lumotlarni to‘plash, ishlatish, saqlash va almashish qoidalarini o‘rnatish.

4. Kuzatuv texnologiyalari orqali olingan ma’lumotlarga kirishni faqat vakolatli xodimlarga berish.

Shuningdek, biz raqamli dunyoda yashayapmiz, hayotimizni internetsiz, virtual olamsiz tasavuur eta olmaymiz. Ma’lumotni saqlash yoki ma’lumotlarga kirish bo‘ladimi, biz bunday ishlarni bajarish uchun internetdan yordam so‘raymiz. Virtual olamni dunyoga tobora ortib borayotgan aralashishi bizni kiber tahdidlarga moyil qilmoqda. Hech shubha yo‘qki, kiber jinoyatlar eksponensial sur'atda o‘sib bormoqda. Internetda foydalangan holda jinoyatchilar yoki xakerlar internet foydalanuvchilarining shaxsiy ma’lumotlariga kirib, ulardan o‘z manfaati uchun foydalanmoqda, tovlamachilik, firibgarlik kabi jinoyatlarni virtual olamda sodir etishmoqda [3].

Statistik ma’lumotlarga ko‘ra, o‘tgan davr mobaynida global sanoatning 85 foizi fishing va ijtimoiy muhandislik kiberhujumlarini boshdan kechirdi [4]. Vaqt o‘tishi bilan kiber hujumlar soni maksimal darajada ortib bormoqda. Innovatsion texnologiyalar va kibermexanizmlarning kiritilishi bilan internet jinoyatchilari har qachongidan ham kuchliroq bo‘lib bormoqda. Ular doimiy ravishda internet olamiga hujum qilib, maxfiy ma’lumotlarni buzmoqda.

Kiberjinoyatchilar doimo oson yondashuvlar orqali katta pul ishlash yo‘llarini izlaydilar. Ularning asosiy maqsadlari cheksiz miqdordagi maxfiy ma’lumotlarga ega bo‘lgan transmilliy kompaniyalar va boy biznesmenlardir. Agar biz o‘ylab ko‘rsak, bizni internetga yaqinlashtiradigan har qanday narsa bizni kiberhujumlarga duchor qilishi mukin.

Hozirda jahon amaliyotida kiber hujumlarning, jinoyatlarning quyidagi bir necha turlari mavjudir:

elektron pochta va internetdan foydalangan holda firibgarlik;
raqamli identifikatsiyani o‘g‘irlash; (o‘g‘irlash va shaxsiy ma’lumotlardan foydalanish);
to‘lov kartasi ma’lumotlarini va boshqa moliyaviy ma’lumotlarni o‘g‘irlash;
korporativ ma’lumotlarni o‘g‘irlash va qayta sotish;
kiber shantaj (hujum tahdidi ostida pul undirish);
ransomware hujumlari (kiber shantajning bir turi);
cryptojacking (boshqa odamlarning resurslaridan foydalangan holda kriptovalyutani qazib olish);
kiber-josuslik (hukumat yoki korporativ ma’lumotlarga ruxsatsiz kirish);
tarmoqni buzish uchun tizimlarning buzilishi;
mualliflik huquqining buzilishi;
noqonuniy qimor o‘yinlari;
taqiqlangan tovarlarning onlayn savdosi;
bolalar pornografiyasini ta’qib qilish, ishlab chiqarish yoki saqlash kabi turlari hozirda ommaga ma’lum hamda rivojlanib bormoqda [5].

Kiberjinoyat har doim quyidagilardan kamida bittasini o‘z ichiga oladi: viruslar yoki boshqa zararli dasturlardan foydalangan holda komputerlarga hujum qilish maqsadida jinoiy faoliyatni amalga oshirish; boshqa jinoyatlarni sodir etish uchun komputer tizimlaridan noqonuniy foydalanish; maqsadlari komputerlarga hujum qilish bo‘lgan kiberjinoyatchilar ularga zarar yetkazish yoki o‘chirish, ma’lumotlarni o‘chirish yoki o‘g‘irlash uchun ularga zararli dasturlarni yuqtirishi kabi usullardan foydalanib sodir etilishi mumkin. Shuningdek, kiberjinoyatchilarning maqsadi DoS hujumi (xizmatni rad etish hujumi) bo‘lishi mumkin, buning natijasida kompaniya foydalanuvchilari yoki mijozlari veb-sayt, komputer tarmog‘i yoki dasturiy ta’minot xizmatlaridan foydalana olmaydi.

Komputerlardan boshqa jinoyatlarni sodir etishda foydalaniladigan kiberjinoyatlar kompyuterlar yoki kompyuter tarmoqlari yordamida zararli dasturlar, taqiqlangan ma’lumotlar yoki tasvirlarni tarqatishga qaratilgan bo‘lishi mumkin. Ko‘pincha kiber jinoyatchilar bir vaqtning o‘zida kompyuterlardan foydalanadilar va ularga hujum qilishadi. Masalan, ular birinchi navbatda virusli kompyuterlarga hujum qilishlari va keyin ularni tarmoq bo‘ylab zararli dasturlarni tarqatish uchun ishlatishlari mumkin. Ba'zi mamlakatlarda kiberjinoyat tasnifi boshqa, uchinchi toifani o‘z ichiga oladi: kompyuterdan jinoyat sodir etishda yordam sifatida foydalanish kabi. Masalan, kompyuterda o‘g‘irlangan ma’lumotlarni saqlash orqali kiberjinoyatchi firibgarlik, tovlamachilik qilib kiber hujum qurbonlaridan pul undirishi, boshqa vositalarni talab qilishi mukin.

Hozirda kiber hujumlarning eng samarali usuli sifatida zararli dastur hujumlari hisoblanmoqda. Bunday holda, kompyuter tizimi yoki tarmog‘i kompyuter virusi yoki boshqa zararli dastur bilan zararlangan bo‘ladi. Shundan so‘ng, kiber jinoyatchilar kompyuterdan maxfiy ma’lumotlarni o‘g‘irlash, ma’lumotlarni buzish va boshqa jinoiy harakatlarni amalga oshirish uchun foydalanishlari mumkin.

Ushbu turdagi kiberjinoyatlarning mashhur namunasi 2017-yilning may oyida WannaCry ransomware dasturidan foydalangan holda global kiberhujumdir. Bunday dasturlar kiberjinoyatchilarga garovga olingan ma’lumotlar yoki qurilmalar uchun to‘lov talab qilish imkonini beradi. WannaCry Microsoft Windows operatsion tizimida ishlaydigan kompyuterlardagi zaiflikdan foydalangan. O‘shanda 150 ta mamlakatdagi 230 000 ta

kompyuter to‘lov dasturidan zarar ko‘rgan. Kiberjinoyatchilar qurbonlari o‘z fayllariga kirish huquqini yo‘qotdilar va kirish huquqini tiklash uchun bitkoinlarda to‘lov talab qilingan xabarni oldilar [6].

O‘zbekistonda ham virtual olamdagi jinoyatlar kundan kunga oshib borayotganiga guvoh bo‘lmoqdamiz. Ma’lumotlarga ko‘ra, yurtimizda 25 mln nafardan ortiq internet foydalanuvchilari mavjud. Mamlakatamizda ham internet bilan foydalanish, kiberjinoyatchilik bo‘yicha doimiy ravishda tadqiqotlar olib boriladi. O‘tkazilgan tahlil natijalari bugungi kunda mamlakatda kiberjinoyatchilikning o‘sish tendensiyasi kuzatilayotganidan dalolat bermoqda.

So‘nggi 3 yilda kiberjinoyatlar soni bir necha baravarga oshib ketgan. Jumladan, kiberjinoyatchilikning bir qator turlari sodir bo‘layotgani kuzatilmoqda. Ular quyidagicha:

1. firibgarlar plastik karta foydalanuvchilariga kelgan SMS-xabarnomadagi kodlarni to‘lovni amalga oshirish, yutuqni berish kabi bahonalar orqali egallab, undagi mablag‘larni o‘zlashtirishi;

2. shaxsiy ma’lumotlarni egallash va ularni oshkor qilish bilan qo‘rqitib tovlamachilik qilishi (kibertovlamachilik);

3. ijtimoiy tarmoqda zo‘rlik ishlatish bilan qo‘rqitishi, haqorat, suitsid holatlari (kiberbulling) va boshqalar hozirda yurtimizdagi kiberjinoyatlarning oshib borayotgan turlari hisoblanadi [7]. Ushbu holatlar milliy qonunchilikni takomillashtirish, davlat tomonidan huquqiy tizimda xalqaro huquqiy normalar ustuvorligini tan olish prinsipi asosida tegishli xalqaro huquqiy normalarga milliy huquq tizimini moslashtirish, ularning mazmunini singdirish hamda kiberjinoyatchilikni oldini olishga qaratilgan xalqaro konvensiya, shartnomalarga qo‘shilishni taqozo etmoqda.

Shunday konvensiyalardan biri 2001-yil 23-noyabrdagi Yevropa Kengashi tomonidan qabul qilingan Kiberjinoyatchilikka qarshi qarshi kurashish bo‘yicha Budapesht konvensiyasidir. Konvensiya internet va boshqa kompyuter tarmoqlari orqali sodir etilgan jinoyatlar to‘g‘risidagi birinchi xalqaro shartnoma bo‘lib, ayniqsa mualliflik huquqining buzilishi, kompyuter bilan bog‘liq firibgarlik, bolalar pornografiyasi va tarmoq xavfsizligini buzish bilan bog‘liq jinoyatlarni oldini olishga qaratilgan shartnomaddir. Shuningdek, u kompyuter tarmoqlarini qidirish va ushlash kabi bir qator vakolatlar va protseduralarni o‘z ichiga oladi.

Kiberjinoyatlar to‘g‘risidagi konvensiya (shuningdek, Kiberjinoyatlar to‘g‘risidagi Budapesht konvensiyasi yoki Budapesht konvensiyasi sifatida ham tanilgan) milliy qonunlarni uyg‘unlashtirish, tergov usullarini takomillashtirish va davlatlar o‘rtasidagi hamkorlikni oshirish orqali internet va kompyuter jinoyatlarini (kiber jinoyatlar) hal qilishga qaratilgan birinchi xalqaro shartnomadir [8].

Konvensiya va uning tayyorlangan hisoboti Yevropa Kengashi Vazirlar Qo‘mitasi tomonidan 2001-yil 8-noyabrdagi 109-sessiyasida qabul qilingan. 2001-yil 23-noyabrda Vengriya poytaxti Budapeshtda imzolash uchun chaqirilgan va 2004-yil 1-iyuldan boshlab kuchga kirgan. 2020-yil dekabr holatiga ko‘ra, 65 davlat konvensiyani ratifikatsiya qilgan, yana to‘rtta davlat konvensiyani imzolagan, ammo uni ratifikatsiya qilmagan ko‘rishimiz mumkin.

Konvensiya internet va boshqa kompyuter tarmoqlari orqali sodir etilgan jinoyatlar to‘g‘risidagi birinchi xalqaro shartnoma bo‘lib, ayniqsa mualliflik huquqining buzilishi, kompyuter bilan bog‘liq firibgarlik, bolalar pornografiyasi, nafrat jinoyatlari va tarmoq

xavfsizligini buzish bilan bog‘liq jinoyatlarga xalqaro tartibda kurasishga kelishuv deb hisoblashimiz mumkin. Shuningdek, u kompyuter tarmoqlarini qidirish, topish, qo‘lga kiritish va qonuniy ravishda jazolash kabi bir qator vakolatlar va tartiblarni o‘z ichiga oladi.

Uning muqaddimada bayon etilgan asosiy maqsadi jamiyatni kiberjinoyatlardan himoya qilishga qaratilgan umumiy jinoiy siyosatni olib borish, ayniqsa tegishli qonun hujjatlarini qabul qilish va xalqaro hamkorlikni rivojlantirishdan iborat.

Konvensiya asosan quyidagilarga qaratilgan:

kiberjinoyatchilik sohasidagi jinoyatlarning milliy jinoiy-moddiy-huquqiy elementlarini va ular bilan bog‘liq qoidalarni uyg‘unlashtirish;

milliy jinoyat-protsessual qonunchiligiga bunday jinoyatlarni, shuningdek, kompyuter tizimi yordamida sodir etilgan boshqa huquqbuzarliklarni yoki ularga tegishli elektron shakldagi dalillarni tergov qilish va jinoiy javobgarlikka tortish uchun zarur bo‘lgan vakolatlarni ta’minlash;

xalqaro hamkorlikning tez va samarali rejimini yaratish kabi ustuvor maqsadlarni ustuvor vazifa qilib qo‘ygan.

Konvensiyada quyidagi jinoyatlar belgilangan: noqonuniy tizimga kirish, noqonuniy qo‘lga olish, ma’lumotlarga aralashuv, tizimga aralashuv, qurilmalardan noto‘g‘ri foydalanish, kompyuter bilan bog‘liq qalbakilashtirish, kompyuter bilan bog‘liq firibgarlik, bolalar pornografiyasi bilan bog‘liq huquqbuzarliklar, mualliflik huquqi va qo‘shni huquqlar bilan bog‘liq huquqbuzarliklardir.

Shuningdek, u saqlangan ma’lumotlarni tezkor saqlash, trafik ma’lumotlarini tezkor saqlash va qisman oshkor qilish, ishlab chiqarish tartibi, kompyuter ma’lumotlarini qidirish va olib qo‘yish, trafik ma’lumotlarini real vaqt rejimida yig‘ish va kontent ma’lumotlarini qo‘lga kiritish kabi protsessual huquqiy masalalarni belgilaydi.

Bundan tashqari, Konvensiyada saqlanadigan kompyuter ma’lumotlariga o‘zaro yordamni talab qilmaydigan transchegaraviy kirishning ma’lum bir turi to‘g‘risidagi qoida mavjud (rozilik bilan yoki hamma uchun mavjud bo‘lganda) va tezkorlikni ta’minlash uchun 24/7 tarmoqni o‘rnatishni nazarda tutadi. Bundan tashqari, shartlar va kafolatlar sifatida Konvensiya inson huquqlari va erkinliklarini, shu jumladan Inson huquqlari to‘g‘risidagi Yevropa konvensiyasi , Fuqarolik va siyosiy huquqlar to‘g‘risidagi xalqaro pakt va boshqa amaldagi inson huquqlari bo‘yicha xalqaro hujjatlardan kelib chiqadigan majburiyatlardan kelib chiqadigan huquqlarni munosib himoya qilishni ta’minlashni talab qiladi va mutanosiblik tamoyilini o‘z ichiga oladi [9].

Konvensiya Yevropa va xalqaro ekspertlarning to‘rt yillik mehnati mahsulidir. U kompyuter tarmoqlari orqali irqchilik va ksenofobiya tashviqotining har qanday nashrini jinoiy tuhmat to‘g‘risidagi qonunlarga o‘xshash jinoiy javobgarlikka tortuvchi qo‘shimcha protokol bilan to‘ldirildi. Hozirda konvensiya doirasida kiberterrorizm ham o‘rganilmoqda.

Budapesht konvensiyasi umumiy standartlar belgilab olgan bo‘lib, Budapesht konvensiyasi jinoiy adolat to‘g‘risidagi shartnoma ham hisoblanadi va u davlatlarga kompyuterlarga qarshi va ular orqali qilingan hujumlar ro‘yxatini jinoiylashtirishni; kiberjinoyatlarni tergov qilish va har qanday jinoyatga oid elektron dalillarni ta’minlashni yanada samaraliroq qilish va qonun ustuvorligi kafolatlarini ta’minlash uchun protsessual huquq vositalari; kiberjinoyat va elektron dalillar bo‘yicha xalqaro politsiya va sud hamkorligini taqdim etadi.

Konvensiyab uni amalga oshirishga va hamkorlik qilishga tayyor bo‘lgan har qanday davlat qo‘shilishi uchun ochiqdir. Konvensiyaning 15 yilligini nishonlagan 2016 yil noyabriga kelib, 50 ta davlat (Yevropa davlatlari, shuningdek, Avstraliya, Kanada, Dominikan Respublikasi, Isroil, Yaponiya, Mavrikiy, Panama, Shri-Lanka va AQSh) ishtirokchi bo‘ldi. Dunyoning barcha mintaqalaridan yana 17 nafari uni imzolagan yoki qo‘shilishga taklif qilingan [10].

Hozirda soni 67 ta bo‘lgan ushbu davlatlar o‘nta xalqaro tashkilot (masalan, Hamdo‘stlik Kotibiyati, Yevropa Ittifoqi, INTERPOL, Xalqaro elektraloqa ittifoqi, Amerika davlatlari tashkiloti, BMTning Narkotiklar va jinoyatchilik bo‘yicha boshqarmasi va boshqalar) a’zo sifatida ishtirok etadilar va Kiberjinoyatlar bo‘yicha konventsiya qo‘mitasidagi kuzatuvchilariga aylanishi mumkin. Ushbu Qo‘mita ahdlashuvchilar tomonidan Konvensiyaning bajarilishini baholaydi va Konvensiyani yangilab turadi. Hozirgi sa'y-harakatlar huquqni muhofaza qilish organlarining bulutli serverlardagi elektron dalillarga kirishiga oid yechimlarga qaratilgan.

Mamlakatimizda ham kiberjinoyatchilikni oldini olish, kiber xavfsizlik tizimlarini rivojlantirish uchun salmoqli ishlar amalga oshirilib kelinmoqda. Kiber xavfsizlikni rivojlantirish maqsadida “Kiberxavfsizlik markazi” DUK tashkil etildi, “Kiberxavfsizlik tg’risida”gi qonun hamda Prezidentimizning 2018-yil 19-fevraldagi “Axborot texnologiyalari va kommunikatsiyalari sohasini yanada takomillashtirish chora-tadbirlari tg’risida”gi Farmoni Hukumatimiz tomonidan raqamli iqtisodiyotni rivojlantirish byicha muhim chora-tadbirlar ishlab chiqilishiga va hayotga tatbiq etilishiga asos bldi. Raqamli ma’lumotlarni boshqarishda axborot xavfsizligini ta’minlash muhim omil sanaladi. Bunda asosiy e’tibor raqamli ma’lumotlarga ruxsatsiz kirish, ularni axborot vositachilaridan himoya qilgan holda xavfsizligini ta’minlash va axborotlar uzatishning soddaligini ta’minlashga qaratilishi lozim.

Mamlakatimiz raqamlashtirish asriga ishonch bilan qadam qydi va bunga hukumat tomonidan qaratilayotgan e’tibor asos bla oladi. Doimiy tarzda amalga oshirilayotgan internet tezligi va sifatini oshirish, zamonaviy axborot-kommunikatsiya texnalogiyalarini hayotimizga tadbiq qilish, axborotlashtirish tizimlarini takomillashtirish bilan birgalikda, hukumat alohida e’tiborni kiberxavfsizlik sohasiga ham qaratmoqda. “Kiberxavfsizlik markazi” davlat unitar korxonasi yurtimizda kiber muhitni xavfsiz va sog’lomligini ta’minlash, axborotlashtirish tizimlarini doimiy va uzluksiz ishlashini qllab quvvatlash, va zararli kiber hujumlardan himoya qilish uchun z oldiga bir qator maqsad va vazifalarni qygan.

rnatilgan maqsad va vazifalarni tlaqonli bajarish uchun Markaz tomonidan milliy internet segmentida axborot va kiberxavfsizlik hodisalarini doimiy monitoring qilib borish ylga qyilgan. Ushbu normativ-huquqiy hujjatlardagi asosiy maqsadlar:

- axborot kommunikatsiya texnologiyalari tizimini zamonaviy kibertahdidlardan himoya qilish, turli darajadagi tizimlar uchun kiberxavfsizlik bo‘yicha zamonaviy mexanizmlarni joriy etish;
- kiberxavfsizlikni ta’minlash sohasida davlat organlari, korxona va tashkilotlarning huquqlari
- va majburiyatlarini belgilash, ularning faoliyatini muvofiqlashtirish; ushbu sohadagi normativ-huquqiy hujjatlarni unifikatsiyalash nazarda tutilishi;
- kiberxavfsizlik sohasidagi vakolatli davlat organi, uning huquq va majburiyatlari;
- davlat organlari va tashkilotlari axborot tizimlari va resurslarining kiberxavfsizligini

ta’minlash bo‘yicha talablarni belgilash;

- kompyuter hodisalariga javob berish – tahdidlarni aniqlash, hujumlar va ularning oqibatlarini aniqlash va oldini olish, ularning oqibatlarini bartaraf etish;
- CeRT (kompyuter hodisalariga javob berish markaz)larning samarali ishlashini ta’minlash;
- muhim axborot infratuzilmasi obektlarining ahamiyatliligi darajasi bo‘yicha me’yoriy huquqiy bazani shakllantirish;
- muhim axborot infratuzilmasi obektlari va subyektlari kiberxavfsizlikni ta’minlashiga doir talablar hamda huquq va majburiyatlari;
- shuningdek, milliy kiberxavfsizlik sohasini rivojlantirish bo‘yicha huquqiy bazani yaratish – mutaxassislar tayyorlash, dasturiy ta’minotlar yaratish nazarda tutilgan.

“Kiberxavfsizlik tg’risida”gi qonunda esa axborot kommunikatsiya va texnologiyalari tizimini zamonaviy kibertahdidlardan himoya qilish, turli darajadagi tizimlar uchun kiberxavfsizlik byicha zamonaviy mexanizmlarni joriy etish, mazkur sohada davlat organlari, korxonalar va tashkilotlarning huquqlari va majburiyatlarini belgilash, ularning faoliyatini muvofiqlashtirish kabilar aks etishi kutilmoqda. Yurtimizda olib borilayotgan barcha islohotlar zamirida xalqimizga qulayliklar yaratish maqsadi yotibdi. Kiberxavfsizlikni ta’minlashga alohida e’tibor qaratilishi raqamli imkoniyatlardan ishonchli va xavfsiz tarzda foydalanishga zamin blib kelmoqda. Iqtisodiyotning barcha sohalarini raqamlashtirish jahon hamjamiyatiga integratsiyalashuv, dunyo bozorida o‘z o‘rniga ega bo‘lish, iqtisodiy ravnaq topish, aholiga qulayliklar yaratish imkoniyatini beradi. Bu esa o‘z navbatida, mamlakatimizda asosiy kun tartibidagi masala hisoblanmoqda. Raqamlashtirish borasida O‘zbekiston dadil odimlar bilan ildamlamoqda. Mamlakatimizda raqamli iqtisodiyotni faol rivojlantirish, barcha tarmoqlar va sohalarda, eng avvalo, davlat boshqaruvi, ta’lim, sog’liqni saqlash va qishloq xjaligida zamonaviy axborot-kommunikatsiya texnologiyalarini keng joriy etish byicha kompleks chora-tadbirlar amalga oshirilmoqda.

Qachonki ko‘plab ma’lumotlar raqamli formatga o‘tkazilsa, elektron ko‘rinishda saqlansa, shundagina axborot va kiberxavfsizlik masalasi dolzarblik kasb etadi. Davlatimiz rahbari tomonidan axborot xavfsizligini ta’minlash sohasi mutaxassislariga shunday talab qo‘yilganki, ular bu borada ro‘y bergan noxush hodisalarni o‘rganishlari va bartaraf etishlari emas, balki bunday holatni oldindan kra bilishlari, ya’ni oldini olishga xarakat qilishlari kerak.

Shuningdek, O‘zbekiston Respublikasi 2001-yil 23-noyabrdagi Yevropa Kengashi tomonidan qabul qilingan Kiberjinoyatchilikka qarshi qarshi kurashish bo‘yicha Budapesht konvensiyasinining standartlarini O‘zbekistonda implementatsiya qilish masalasini ko‘rib chiqilishi maqsadga muvofiq bo‘ladi. Konvensiyaga qo‘shilish mumkin hamda u barcha mamlakatlar uchun ochiqdir. Konvensiya qoidalariga ko‘ra, Konvensiya kuchga kirgandan keyin Yevropa Kengashi Vazirlar Qo‘mitasi maslahatlashuvlar va Konvensiya ishtirokchi-davlatlarining bir ovozdan roziligidan so‘ng Yevropa Kengashiga a’zo bo‘lmagan har qanday davlatni ushbu Konvensiyaga qo‘shilish uchun uni ishlab chiqishda ishtirok etmagan bo‘lsa ham taklif qilishi mumkin. Bunday qaror Yevropa Kengashi Nizomining 20^{d}-moddasida nazarda tutilgan ko‘pchilik ovoz bilan, Vazirlar Qo‘mitasiga a’zo bo‘lish huquqiga ega bo‘lgan ahdlashuvchi tomonlar vakillarining bir ovozdan roziligi bilan qabul qilinadi [11].

Shuningdek, Konvensiya 1-bandga muvofiq, Konvensiyaga qo‘shilgan har qanday

davlatga nisbatan Konvensiya Bosh kotibga saqlash uchun topshirilgan kundan keyin uch oylik muddat o‘tgandan keyingi oyning 1-kunida kuchga kiradi.

Konvesniya a’zo mamlakatlarga ba’zi hamkorlik bilan bog‘liq majburiyatlarni vujudga keltiradi. Masalan, Tomonlar qoidalariga muvofiq, jinoyat ishlari bo‘yicha xalqaro hamkorlik to‘g‘risidagi tegishli xalqaro hujjatlarni, yagona yoki o‘zaro qonunchilikka asoslangan kelishilgan kelishuvlarni va ichki qonunchilikni qo‘llash orqali to‘liq hajmda hamkorlik qiladilar, tergov yoki sud jarayoni, kompyuter tizimlari va ma’lumotlari bilan bog‘liq jinoiy huquqbuzarliklar bo‘yicha jinoiy ish qo‘zg‘atish yoki jinoiy huquqbuzarlik dalillarini elektron shaklda to‘plash kabi huquqiy yordamlarni amalga oshiradi. 2001-yil 23-noyabrdagi Yevropa Kengashi tomonidan qabul qilingan Kiberjinoyatchilikka qarshi qarshi kurashish bo‘yicha Budapesht konvensiyasinining standartlarini O‘zbekistonda implementatsiya qilish uchun hukumat milliy axborot xavfsizligini rivojlantirish, xalqaro mamlakatlar so‘rovlariga va konveniya bo‘yicha yordamlarni o‘z vaqtida amalga oshirish qobiliyatiga ega bo‘lishi lozim. Ahdlashuvchi tomonlar kiberjinoyatchilarga vaaqtinchalik choralar ko‘rish bilan bog‘liq, tergov vakolatlari bilan bog‘liq yordamlar bo‘yicha o‘zaro so‘rovlar yuborishi huquqiga ega bo‘ladi.

Lekin, 2001-yil 23-noyabrdagi Yevropa Kengashi tomonidan qabul qilingan Kiberjinoyatchilikka qarshi qarshi kurashish bo‘yicha Budapesht konvensiyasi muammoli jihatlari ham mavjud. Ba’zi mamlakatlar rasmiy vakillari Kiberjinoyatchilik bo‘yicha Budapesht konvensiyasini eskirgan deb hisoblashini bildirishgan.

Rossiya Tashqi ishlar vazirligining yangi chaqiriqlar va tahdidlar departamenti direktori Ilya Rogachevning so‘zlariga ko‘ra, kelishuvda ko‘plab kamchiliklar mavjud. “Budapesht kiberjinoyat konvensiyasi eskirgan va qayta ko‘rib chiqilishi kerak”. Bu haqda 4-dekabr kuni Rossiya tashqi ishlar vazirligining yangi chaqiriqlar va tahdidlar departamenti direktori Ilya Rogachev Internet boshqaruvi bo‘yicha IV Jahon konferensiyasida so‘zlagan nutqida ma’lum qildi.

Yevropa Kengashi 2001-yilda qabul qilingan Kiberjinoyatchilik bo‘yicha Budapesht konvensiyasini ishlab chiqish orqali maqbul va qonuniy asosli mexanizm yaratishga birinchi urinish bo‘lgan bo‘lsada, bu kelishuv juda ko‘p muhim kamchiliklarga egaligini konvensiyadagi normalar orqali tadqiq qilishimiz mumkin.

Birinchidan, u 1997-2001-yillarda, axborot-kommunikatsiya texnologiyalari sohasidagi jinoyatlar juda oddiy bo‘lgan paytda tayyorlangan edi.

O‘sha yillarda zamonaviy botnetlar (katta zararli harakatlarni amalga oshirish uchun internet orqali boshqariladigan kompyuterlar – TASS) kabi murakkab muammolar bo‘lmaganini hisobga olishimiz lozim. Shuningdek, konvensiya kiberjinoyatlarning keng tarqalgan spam va onlayn firibgarlik kabi hozirgi ko‘rinishlariga adekvat javob berilmagan.

Shuningdek, Konvensiya bilan bog‘liq asosiy to‘siqlardan yana biri, Budapesht konvensiyasi 32-moddaning “B” bandi mazmuni bo‘lib, uning mazmuni ba’zi qonunchilik normalariga zid bo‘lishi mumkin. Xususan, hujjatning ushbu qismiga muvofiq, mexanizm ishtirokchilari tegishli ma’lumotlarga ega bo‘lgan davlat organlarini xabardor qilmasdan, boshqa tomonning egaligidagi ma’lumotlarga transchegaraviy kirish huquqini oladi deyilgan qism mavjud bo‘lim ushbu holat, bu bilan Budapesht konvensiyasi asosiy fuqarolik huquqlarining, bu birinchi navbatda shaxsiy ma’lumotlarga tegishli qismlarni buzilishiga yo‘l qo‘yishi mumkinligini anglatadi.

O‘zbekiston axborot-kommunikatsiya texnologiyalaridan jinoiy maqsadlarda foydalanishga qarshi kurash olib boradigan asosiy tamoyillarga amal qiladi, chunki bu muammo global xarakterdagi, xususan, transchegaraviy jinoiy faoliyatning eng muhim muammolaridan biriga aylandi. Biz katta moddiy zarar bilan birga ularning soni ortib borayotganini ko‘ryapmiz.

Ushbu hujjat Internet tarmog‘ida jinoyatlarga qarshi kurashni amalga oshirishda turli davlatlarning harakatlarini tartibga solish imkonini bersada, O‘zbekiston Respublikasi kompyuter tarmoqlari faoliyatiga rasmiy xabarnomasiz aralashish imkoniyati mavjudligi, davlatning xavfsizligi va suverenitetiga tahdid solishi mumkin. Konvensiyani qabul qilish bilan bog‘liq foydali va muammoli jihatlar yanada ko‘proq o‘rganilishi va tadqiqotlar olib borilishi maqsadga muvofiqdir.

Shunday bo‘lsada, ushbu hujjat texnologik salohiyat, hukumatlar va xizmat ko‘rsatuvchi provayderlar o‘rtasidagi hamkorlik nuqtai nazaridan oldinga katta qadam bo‘lganidan dalolat beradi. Bu kibermakonda qonun ustuvorligini mustahkamlaydi, foydalanuvchilarni himoya qiladi va onlayn jinoyat qurboni bo‘lganlar uchun adolatni ta’minlashga yordam beradi.

Kiberjinoyatlarning keng tarqalishi va xorijiy, ko‘p, o‘zgaruvchan yoki noma’lum yurisdiksiyalarda joylashgan bo‘lishi mumkin bo‘lgan elektron dalillarni olishning murakkablashishi bilan huquqni muhofaza qilish organlarining vakolatlari hududiy chegaralar bilan cheklanadi. Natijada, davlatlarning vakolatli organlariga ma’lum bo‘lgan kiberjinoyatlarning faqat kichik bir qismi bilan kurashish mumkin bo‘lib qoladi. Bunga qarshi turish uchun xalqaro shartnomalarga qo‘shilish, hukumatlararo o‘zaro yordamning yo‘lga qo‘yilishi kiberjinoyatlarga qarshi samarali kurashishda muhim ro‘l o‘ynaydi.

Xulosa o`rnida shuni aytib o`tish joizki, yurtimizda kiberxafvsizlikni yaxshilash uchun quyidagi takliflarimni berib o`tmoqchiman.

**1.Mavjud qonunchilikdagi bo`shliqlarni aniqlash va yangilash:** Kiberxavfsizlik bo`yicha qonunchilikni takomillashtirishning birinchi bosqichi bo`shliq va kamchiliklarni aniqlash uchun amaldagi qonun va me`yoriy hujjatlarni qayta ko`rib chiqishdan iborat. Bo‘shliqlar aniqlanishi kerak.

2. Ogohlikka chaqirish va ta'lim berish orqali kiberxafvsizlikni oshirish: Kiberxavfsizlik nafaqat hukumatning, balki shaxslar va tashkilotlarning ham amalga oshirishi kerak bo`lgan vazifalaridan biri hisoblanadi. Shu bois keng jamoatchilik, korxonalar va davlat amaldorlari o`rtasida kiberxavfsizlik bo`yicha xabardorlikni oshirish va ta`limni kuchaytirish zarur.

3. Milliy kiberxavfsizlik strategiyasini yaratish: Kiberxavfsizlikning keng qamrovli milliy strategiyasi barcha manfaatdor tomonlarning kibert ahdidlarga qarshi birgalikda ishlashi uchun ishlab chiqilishi kerak.

4. Kiberxavfsizlik agentligini tashkil etish: Milliy kiberxavfsizlik strategiyasini muvofiqlashtirish va amalga oshirish uchun kiberxavfsizlik uchun mas'ul bo‘lgan markazlashtirilgan agentlik tashkil etilishi kerak. Ushbu agentlik kibertahdidlarni samarali hal qilish uchun yetarli darajada xodimlar va resurslar bilan ta'minlanishi kerak.

5. Axborot almashishni yaxshilash: Samarali kiberxavfsizlik uchun turli manfaatdor tomonlar o‘rtasida ma’lumot almashish muhim ahamiyatga ega. Shu sababli, davlat idoralari, xususiy kompaniyalar va boshqa manfaatdor tomonlar o‘rtasida tahdidlar haqidagi razvedka

va kiberxavfsizlik ma'lumotlarini almashishni rag'batlantirish va himoya qilish uchun qonunlar ishlab chiqilishi kerak.

6. Kiberxavfsizlik hodisalariga javob rejasini ishlab chiqish: Hodisalarga javob berish rejasi kiber hodisalarga javob berish uchun asos yaratish uchun ishlab chiqilishi kerak. Reja hodisalar haqida xabar berish, hodisalarni tekshirish va hodisalardan tiklanish tartiblarini o'z ichiga olishi kerak.

7. Davlat-xususiy sheriklikni rag'batlantirish: Davlat-xususiy sheriklik kiberxavfsizlikni yaxshilashda samarali bo`lishi mumkin. Hukumat kiberxavfsizlik siyosati va tashabbuslarini ishlab chiqish va amalga oshirish uchun xususiy sektor bilan hamkorlik qilishi kerak.

Иқтибослар/Сноски/References:

1. https://tashviqot.uz/index.php/2022/10/04/2506/
2. https://library-tsul.uz/viktimologiya-rustambayev-m-x-niyozova-s-s-2021
3. https://www.jigsawacademy.com/blogs/cyber-security/major-causes-of-cyber-crimes-you-must-be-aware-of/
4. https://earthweb.com/cybercrime-statistics/
5. https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime
6. https://www.kaspersky.com/resource-center/threats/ransomware-wannacry
7. https://zamon.uz/detail/ozbekistonda-songgi-3-yilda-kiberjinoyatlar-keskin-oshgan-ozbekiston
8. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185
9. Convention on Cybercrime, Article
10. https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building/
11. https://base.garant.ru/4089723/9db18ed28bd6c0256461e303941d7e7a/#block_3701
12. https://tass.ru/politika/4782506