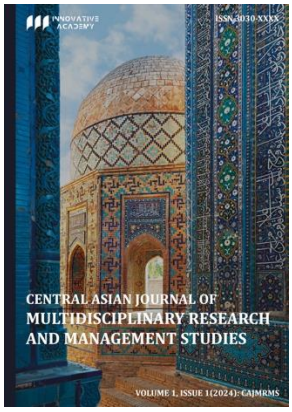

KIBERXAVFSIZLIKNING ICHKI ISHLAR ORGANLARI TIZIMIDAGI O‘RNI VA KIBERJINOYATLARNI OLDINI OLISHDAGI AHAMIYATI

Sayfullayev O‘lmasjon Shavkat o‘g‘li
O‘zbekiston Respublikasi Ichki ishlar vazirligi akademiyasi mustaqil izlanuvchisi
Mamatjonov Jahongir Tursunali o‘g‘li
O‘zbekiston Respublikasi Ichki ishlar vazirligi akademiyasi kursanti
https://doi.org/10.5281/zenodo.11523628

ARTICLE INFO

Received: 01st June 2024
Accepted: 03th June 2024
Published: 06th June 2024

KEYWORDS

Kiberxavfsizlik, kiberjinoyat, kibertahdidlar, internet, axborot texnalogiyalari, kiberhujum, clouds (bulutlar), kibermakon , Ichki ishlar organlari, kibertahdid, kiberjinoyatchi

ABSTRACT

Ushbu maqolada kiberxavfsizlikning Ichki ishlar organlari tizimidagi o’rnini va kiber jinoyatlarni oldini olishga qaratilgan ma’lumotlar berilgan. Kiberxavfsizlik internetga ulangan tizimlarni, jumladan qurilma, dasturiy ta’minot va ma’lumotlarni kiberhujumlardan himoya qilishni nazarda tutadi. Bunda, asosan, tahdidlarni va zaifliklarni kamaytirish, xalqaro hamkorlik va kompyuter tarmog’i operatsiyalari, axborotni ta’minlash va huquqni muhofaza qilish kabi harakatlarni qamrab olish uchun hamkorlik qiladigan odamlar, jarayonlar va texnologiyalar haqidagi ma’lumotlar yoritilgan.

Bugungi kunda global axborot maydonida kiber makon bilan bog‘liq yangidan-yangi tahdidlar yuzaga kelmoqda. Shu bois virtual olamdagi hujumlardan himoyalanish masalasi dunyo hamjamiyatini jiddiy tashvishga solmoqda. Raqamli ekotizimga tayanadigan bugungi texnologik rivojlangan davrda kiberxavfsizlik bo'yicha mustahkam chora-tadbirlarni ta'minlash zarurati muhim ahamiyatga ega. Kibertahdidlar tabiatan turlicha bo‘lib, o‘zaro bog‘langan tizimlarimizdagi zaifliklardan foydalanishga doimo intilayotgan zararli shaxslar soni ortib bormoqda. Kiberxavfsizlik landshafti doimo yangi tahdid va muammolarga moslashib, rivojlanib boradi. Korxonalar, jismoniy shaxslar va tashkilotlar uchun o'zlarining kiberxavfsizlik amaliyotlarida xabardor va faol bo'lishlari juda muhimdir. Kiberxavfsizlik sohasidagi muhim jihatlarni o‘rganib chiqib, biz xavf-xatarlarga samarali qarshi tura olamiz va raqamli himoyamizni mustahkamlay olamiz.

Bugungi kunda mamlakatimizda fuqarolarimizni uzog‘ini yaqin qilishga, yashash sharoitlarini zamonaviy shaklda o‘zgartirishga qaratilgan sog‘lom Internet-muhitiga ega axborotlashgan jamiyatni rivojlantirishga alohida e'tibor qaratilgan. Shu munosabat bilan O‘zbekiston Respublikasida “Raqamli O‘zbekiston-2030” dasturini ishlab chiqilishi va hayotga tatbiq etilishi, eng avvalo, puxta va mukammal tashkiliy-huquqiy mexanizmlarni shakllantirish, qolaversa, innovatsion g‘oyalar, texnologiyalar va ishlanmalarni joriy etish bo‘yicha davlat organlari va tadbirkorlik sub’ektlarining uzviy hamkorligini ta’minlash, barcha soha va tarmoqlarda ishlab chiqarish va xizmat ko‘rsatishni raqamli texnologiyalar bilan qamrab olish, bu borada zamonaviy bilimlarni chuqur egallagan, intellektual salohiyatli

kadrlarni yetishtirish, shu orqali, mamlakatda “xavfsiz axborotlashgan jamiyat” muhitini yaratishga xizmat qiladi. Internet tarmoqlaridan foydalanib sodir etiladigan huquqbuzarliklarning barvaqt oldini olish masalasida qonunchilikda belgilab berilgan huquqbuzarliklar profilaktikasining barcha turlari va ularning chora-tadbirlaridan samarali foydalanish lozim. Ichki ishlar organlarini kiberxavsizlikni ta'minlash va kiberjinoyatlarni sodir etilishini profiliktikasi, ularni oldini olish borasida O‘zbekiston Respubikasining “Huquqbuzarliklar profilaktikasi to‘g‘risida”gi Qonuni bilan profilaktikasining turlari belgilab berilgan. Shuningdek, O'zbekiston Respublikasi Qonuni 15.04.2022-yildagi O'RQ-764-son “Kiberxavfsizlik to'g'risida”gi qonunida kibermakonda shaxs, jamiyat va davlat manfaatlarini ta’minlash, kiberjinoyatni sodir etgan shaxslarga nisbatan qo'llaniladigan jazolar haqida gap boradi.

“*Kiberxavfsizlik” - internetga ulangan tizimlarni, jumladan qurilma, dasturiy ta’minot va ma’lumotlarni kiberhujumlardan himoya qilishni anglatadi.* Bunda, asosan, tahdidlarni va zaifliklarni kamaytirish, xalqaro hamkorlik va kompyuter tarmog’i operatsiyalari, axborotni ta’minlash va huquqni muhofaza qilish kabi harakatlarni qamrab olish uchun hamkorlik qiladigan odamlar, jarayonlar va texnologiyalar tushiniladi. Bu tarmoqlar, qurilmalar, dasturlar va ma’lumotlarga hujumlar, o’g’irlik, zarar, modifikatsiya yoki ruxsatsiz kirishning oldini olishga qaratilgan texnologiyalar, usullar va amaliyotlar to’plamidir. Kiberhujumlar global muammoga aylanmoqda. Bu jahon iqtisodiyotiga tahdid solishi mumkin bo‘lgan ko‘plab qo‘rquvlarni keltirib chiqardi. Kompaniyalar va tashkilotlar, xususan, milliy xavfsizlik, sog’liqni saqlash yoki moliyaviy ma’lumotlar bilan bog‘liq ma’lumotlar bilan shug‘ullanuvchilar o‘zlarining maxfiy biznes va shaxsiy ma’lumotlarini kiberhujumlardan himoya qilish uchun harakat qilishlariga zarurat tug‘ilmoqda. Kompyuterlar, tarmoqlar, ilovalar va ma’lumotlar xavfsizligini ta’minlash uchun samarali kiberxavfsizlik strategiyasida bir nechta himoya qatlamlari qo‘llaniladi. Kibertahdidlarga qarshi muvaffaqiyatli mudofaani yo‘lga qo’yish uchun tashkilot xodimlari, jarayonlari va texnologiyasi bir-birini qo’llab-quvvatlashi va to’ldirishi kerak bo’ladi.

Kiberxavfsizlik kelajagida ortib borayotgan kiberhujumlar mavjud. Jismoniy shaxs yoki tashkilot qasddan va yovuz niyatda boshqa shaxs yoki tashkilotning axborot tizimiga kirishga urinsa, bu kiberhujum deb ataladi. Aksariyat hujumlar iqtisodiy maqsadga ega bo‘lsa-da, hozirda amalga oshirilayotgan bir nechta operatsiyalar maqsad sifatida ma’lumotlarni yo‘q qilishni o‘z ichiga olmoqda. Yomon niyatli shaxslar ko‘pincha to’lov yoki boshqa moliyaviy daromad olish usullarini izlaydilar, ammo hujumlar turli sabablarga ko‘ra amalga oshirilishi mumkin, jumladan, siyosiy harakatlar. Kiberxurumlar kelajakda kiberxavfsizlikda hal qilinishi kerak bo’lgan asosiy masala bo’ladi. Kelajakda Clouds (Bulutlar) hujum ostida bovlishi mumkin. Ommaviy bulutli domenlarning ommaviyligi ortib borayotgani platforma resurslari va muhim ma’lumotlarga qaratilgan kiberhujumlarning ko‘payishiga olib keldi. 2018-yilda bo‘lgani kabi, bulutli resurslarning noto‘g‘ri konfiguratsiyasi va noto‘g‘ri boshqarilishi 2019-yilda ham bulutli ekotizim uchun eng xavfli bo‘lib qoldi. Natijada, ta’sirlangan bulutli aktivlar keng doiradagi hujumlarga duchor bo‘ldi. Bulutli infratuzilmalarni noto‘g‘ri sozlash joriy yilda butun dunyo bo’ylab korxonalar zarar ko‘rgan ko‘plab ma’lumotlarni o‘g‘irlash hodisalari va hujumlarining asosiy sabablaridan biri bo’ldi. Docker xostlari fosh qilindi va raqobatchilarning bulutga asoslangan kripto qazib olish faoliyati to‘xtatildi. Check Point tadqiqotchilarining fikricha, ommaviy bulut infratuzilmalariga qarshi ekspluatatsiyalar soni ham oshgan.

Kiberxavfsizlik xodimlari bir necha kiberhujumlarga qarshi kurashishi lozim. Bularga bir necha misol keltirsam: *Fishing* – bu kiberhujumning keng tarqalgan usuli bo'lib, kelajakda ham kiberxavfsizlikning eng jiddiy xavflaridan biri bo'lib qolmoqda. Elektron pochta xavfsizligi mexanizmlari ilg'or darajadagi ijtimoiy muhandislikdan qochish taktikasi tomonidan zarar ko'rmoqda. *Check Point* tahlilchilariga ko'ra, tovlamachilik sxemalari va biznes elektron pochta kelishuvi (BEC) ko'payib bormoqda, ular qurbonlarni shantaj bilan tahdid qilish yoki to'lovni olish uchun boshqalarga taqlid qilish orqali tahdid qilmoqda. Ikkala firibgarlik ham har doim ham zararli qo'shimchalar yoki havolalarni o'z ichiga olmaydi, bu esa ularni aniqlashni qiyinlashtiradi. Bir marotaba qandaydir harakatlar Markaziy razvedka boshqarmasi sifatida namoyon bo'ldi va qurbonlarni aprel oyida bolalar haqidagi ba'zi noqonuniy videolarni tarqatish va saqlashda gumon qilinganligi haqida ogohlantirdi. Bir guruh hakerlar esa Bitcoin uchun 10 000 dollar talab qilishdi. Kiberxavfsizlik kelajagida mobil qurilmalarga hujumlar kuchaymoqda. Kiberhujumchilar mobil dunyoga tahdid landshaftining umumiy modellari va usullarini joriy qilmoqdalar. 2018-yil bilan solishtirganda, banklarga oid zararli dasturlar mobil kiber arenaga muvaffaqiyatli kirib keldi va ularning keskin o'sishi 50% dan oshdi. Jabrlanuvchilarning bank hisoblaridagi to'lov ma'lumotlari, hisob ma'lumotlari va mablag'larini o'g'irlashi mumkin bo'lgan zararli dastur keng tahdidlar muhitidan chiqarib yuborildi va banklarning mobil ilovalaridan ko'proq foydalanish natijasida ayniqsa keng tarqalgan mobil tahdidga aylandi. Kiberxavfsizlik kelajagida ransomware hujumlarining kuchayishi kutilmoqda. *Ransomware* so'nggi yillarda ancha mashhur bo'ldi. Kichik mahalliy va shtat hukumat idoralari, birinchi navbatda, AQShning janubi-sharqida nishonga olingan. Bulutli hisoblash, bulutga asoslangan obuna xizmatlari va mobil qurilmalarning tez tarqalishi an'anaviy tarmoq perimetrlarini zaiflashtirmoqda. Vektorlar soni ortib borishi bilan kompaniyalarga hujum qilish usullari ham ortadi. Shu kabi Kiberjinoyatlarga qarshi kurashishda Ichki ishlar organlari xodimlarini mehnati katta hisoblanadi.

Mutaxassislarning fikricha, kiberxavfsizlikning kelajagi 2025-yilga borib 170 milliard dollarlik sektorgacha o'sadi. So'nggi besh yil davomida kiberxavfsizlik bo'yicha mutaxassislar o'rtacha IT-mutaxassisdan ko'proq pul ishlab topdilar. Farq bo'yicha o'rtacha daromad nomutanosibligi 9% ni tashkil qiladi. Mavjud ish o'rinlari soni ortib borayotgan va ish haqi yaxshilanayotgan bo'lsa-da, malakalar bo'shlig'ini yopish uchun ko'proq vaqt talab etiladi. Kiberxavfsizlikni o'rgatuvchi ta'lim markazilari ma'lumotlariga ko'ra, agar kiberxavfsizlik bo'yicha ish izlovchilar malaka oshirishni boshlamasa, *2025-yilga borib sektorda 1,8 million kiberxavfsizlik bo'yicha mutaxassis yetishmaydi.* Kiberjinoyatlarning kun sayin ortib borishi bilan bu kasbga bo'lgan talab ham oshadi. Bu qiyin, ammo juda foydali ishga aylanadi. Kiberxavfsizlikning qiyinchiliklari kundan-kunga kengayib, rivojlanib borayotganligi sababli, kiberxavfsizlik bo'yicha malakali mutaxassislarga butun dunyo bo'ylab talab katta. Kiberjinoyatchilarning tobora takomillashgan strategiyalari firmalarga zarar yetkazishda davom etar ekan, kiberxavfsizlik barcha turdagi korxonalar uchun ortib borayotgan tashvishga aylanib bormoqda. *Gartner ma'lumotlariga ko'ra,* firmalar 2025-yilda xavfsizlikka 123 milliard dollardan ortiq mablagv sarflaydi, 2022-yilda bu ko'rsatkich 170,4 milliard dollarga yetishi kutilgandi. Ushbu sohadagi ajoyib iste'dodlar uchun kompaniyalar 1,5 milliondan 4 milliongacha pul to'lashga tayyor. Har bir kompaniya o'z ma'lumotlarini himoya qilish uchun kiberxavfsizlik bo'yicha mutaxassislarga muhtoj bo'lganligi sababli, deyarli har

bir sohada son-sanoqsiz ish o‘rinlari mavjud bo‘ladi. Kiberxavfsizlik bo‘yicha mutaxassislar o‘z tashkiloti ma‘lumotlarining xavfsizligini ta’minlash uchun mas’uldirlar.

So‘nggi yillarda IT-sanoati ko‘plab mamlakatlar iqtisodiy farovonligiga katta hissa qo‘shdi. Talab qilinadigan ko’nikmalar: Birinchi va eng muhim talab – bu sohaga kuchli qiziqish. Kiberxavfsizlik bo’yicha lavozimlarga nomzodlar kuchli qiziqish hissi va unga nisbatan kuchli ishtahaga ega bo’lishi kerak. Kiber tahdid landshafti doimo o’zgarib turadi, shuning uchun agar siz ushbu sohaga qiziqsangiz, o’rganishni davom ettirishga va kuch sarflashga tayyor bo‘lishingiz kerak. Quyida yangi boshlovchilar muvaffaqiyatli kiberxavfsizlik karyerasini boshlashlari kerak bo’lgan kiberxavfsizlik ko’nikmalari keltirilgan: *Tarmoqqa ulanish.* Tarmoq – bu bizning ro’yxatimizdagi dastlabki kiberxavfsizlik mahoratidir. Kompyuter tarmoqlarda muntazam tranzaksiyalar va aloqa xavfsizlikni talab qiladi. Kundalik faoliyatida korxonalar turli tarmoqlardan foydalanadilar. Lokal tarmoqlarni (LAN), keng maydon tarmoqlarini (WAN) va virtual xususiy tarmoqlarni (VPN) boshqarish uchun qanday sozlashni o’rganish juda muhimdir. Kodlash – bu dasturiy ta’minot yaratish uchun ishlatiladigan kompyuter dasturlash tili. HTML va Javascript kabi tillarda kodlashning asosiy tushunchalarini tushunish ularning kiberhujumlarga nisbatan zaifligini yaxshiroq tushunishga yordam beradi. *Tizimlar va ilovalar* Dasturiy ta’minot va tizimlarni bilish kiberxavfsizlikning yana bir muhim mahoratidir. Kompyuter dasturlari va boshqa ilovalar kompaniyaning muhim vositalari bo‘lganligi sababli, ular haqida hamma narsani tushunish zarurdir. Agar siz qanday qilib ishga tushirishni va ma’lumotlar bazalari va veb-serverlarni saqlashni o‘rgansangiz, zaifliklarni aniqlash orqali ilovalar xavfsizligini yaxshilashga tayyor bo’lasiz. *Turli sohalarda IT bilimlari* Texnologiyaning asosini tashkil etuvchi tizimlar va jarayonlarni tushunish uchun IT haqida o‘rganish kerak. Aqlli kiberxavfsizlik bo‘yicha mutaxassis baxtsiz hodisalar qanday sodir bo‘lishini va ularni qanday qilib oldini olishni biladi. Tizimlarni yaxshi tushunish yana bir muhim kiberxavfsizlik mahoratidir. Umumiy operatsion tizimlarning o‘ziga xos xususiyatlarini o’rganish va mobil tizimlar haqida hamma narsani bilish uchun *Linux Terminal* yoki *Windows Power shell* kabi buyruq qatori interfeyslari bilan tanishish lozim. *Texnologik innovatsiyalar.* Biz kiberhujumchilarni yoqtirmaymiz, lekin ularga bitta narsani berishimiz kerak: *haqiqiy innovator ruhi*. Biz o‘zimizni himoya qilishga tayyor bo‘lishimiz uchun yangi texnologiya va ularning rivojlanishidan xabardor bo‘ishimiz kerak. Kiberxavfsizlik innovatsiyalari tijorat tarmoqlariga zararli hujumlardan himoyalanish uchun yangi asoslarni qurmoqda. “Covid-19” inqirozi davrida yangi ish muhitlarining qabul qilinishi kiberxavfsizlikning ahamiyatini avvalgidan ham ko‘proq ko‘rsatdi.

Kiberxavfsizlik innovatsiyalari ushbu sohada muhim yutuqlarni keltirib chiqardi. Biz raqamli imkoniyatlarga ega kelajak sari intilayotganimiz sababli, kiberxavfsizlik bo‘yicha mutaxassislar tasavvurga ega bo‘lishlari va yangi g‘oyalarni hayotga tatbiq etishlari muhim. Kiberxavfsizlik kelajagidagi ish o’rinlari va imkoniyatlar Kelajakda kiberxavfsizlik bo‘yicha ish imkoniyatlari juda ajoyibdir. Bu haqida o‘ylab ko‘rsak, kiberxavfsizlik bo’yicha bandlikning o‘rtachadan yuqori o‘sishi juda mantiqiy bo‘ladi. Texnologiya har bir insonning kundalik hayotiga tobora ko‘proq kirib borar ekan, kiberxavfsizlik bo‘yicha professional mutaxassislarga talab ortib boradi. Kiberxavfsizlik maoshlari ham yuqori va kundan-kunga ortib bormoqda. Kelajakda kiberxavfsizlik bo’yicha ish bilan ta’minlash bo‘yicha hisob-kitoblar ko‘proq imkoniyatlarni ko‘rsatsa-da, haqiqat shuki, hozir bu sohada ishlash uchun yetarli malakali mutaxassislar soni juda kam. Malakali kadrlar tanqisligi tufayli kiberxavfsizlik

bo'yicha kasbni tanlaganlar ko'plab imkoniyatlar, yaxshi daromad va ajoyib imtiyozlarni kutishlari mumkin. Kiberxavfsizlik sohasida Ichki ishlar vazirligining "Kiberxavfsizlik markazi" xodimlari faoliyat yuritmoqdalar. Malakali xodimlar yurtimizda va virtual olamda sodir bo'layotgan kiberhujumlarga qarshi kurashmoqda. Har yili ushbu markaz va Respublikaning turli hududlarda kiberjinoyatlarga qarshi kurashish uchun Ichki Ishlar Vazirligi Akademiyasi bitiruvchilari o'z faoliyatlarini boshlashadi. Kiberxavfsizlik sohasida tahsil oluvchi kursantlar ta'lim jarayonida, turli kiberhujumlarga qarshi kurashish uchun o'z bilimlarini rivojlantirishadi. Shu bilan bir qatorda, Toshkent axborot texnologiyalari universiteti hamda boshqa oliygoh bitiruvchilari bu sohada faoliyat yuritadi.

Kiberjinoyat - bu chegarasiz jinoyat bo'lib, uning oqibatlari va oqibatlari cheksizdir; Birlashgan Millatlar Tashkilotining Xavfsizlik Kengashi ko'plab davlatlarni qiynayotgan ushbu kiberjinoyatlarning oqibatlarini boshqarish va yumshatish uchun xalqaro qonunlarni yaratishda muhim rolga ega bo'lishi kerak. Ikkinchi jahon urushi oxirida xalqaro tinchlikni saqlash uchun Xavfsizlik kengashini tashkil etish zarurati tug'ildi. Biroq, 1945 yilda asosiy tashvish bir mamlakatning boshqasiga bostirib kirishining oldini olish uchun qurolli qo'shinga ega bo'lish edi. Ammo texnologiya yutuqlari, ixtiro va Internetning keng qo'llanilishi bilan barcha davlatlarga qarshi yangi tahdid paydo bo'ldi - bu yerdagi qo'shinlar bilan kurashish mumkin emas. Xavfsizlik Kengashi kiber-urush, kiber-terrorizm va boshqa kiberharakatlardan kelib chiqadigan tahdidlarga qarshi kurashish uchun kiberxavfsizlik bo'yicha xalqaro siyosatni amalga oshirish bo'yicha vakolatli organ hisoblanadi.

Kiber-jinoyatchilik nisbatan yangi tushuncha bo'lsada, ko'plab davlatlar iqtisodiyotiga qimmatga tushayotgan muammo. Jinoyat quroli – internet va eng so'nggi raqamli texnologiyalar. Mamlakatning harbiy, strategik tarmoqlarini ishdan chiqarish salohiyatiga ega. Buzg'unchi-xakerlarni topib jazolash esa oson ish emas, chunki ular davlatdan doimo bir qadam oldinda. Bugungi hayotni zamonaviy texnologiyasiz tasavvur qilish qiyin. Uyali aloqa va internet dunyosidagi so'nggi kashfiyotlar uzoqni yaqin, og'irni yengil, biznes imkoniyatlarni esa kengaytirgan. Biroq bu qulayliklar boshqa bir sohaga e'tibor qaratmoqda. Kiber-xavfsizlik har bir davlat uchun alohida strategik masaladir. "Avval asosan davlat sirlari va yuqori texnologiyalar nishonga olingan bo'lsa, hozir jinoyatchilar mo'ljalni kengroq olmoqda", deydi AQSh Federal Qidiruv Byurosi (FBR) rahbari Robert Myuller.

O`zbekistonda ham so`nggi uch yilda bu turdagi jinoyatlar 8,3 baravarga ko`payib, hozirda umumiy jinoyatchilikning qariyb 5 foiziga etgan. Xususan, noqonuniy bank-moliya operasiyalari orqali o'zgalarning plastik kartadagi mablag'larini o'zlashtirish, zararli viruslar tarqatish, qimor va tavakkalchilikka asoslangan onlayn o'yinlar, diniy aqidaparastlikka qaratilgan axborot xurujlari, onlayn savdo maydonidagi firibgarlik jinoyatlari ko'payib bormoqda. Mamlakatda 2020-yilda axborot texnologiyalari sohasida 106 ta jinoyat qayd etilgan. 2021-yilda bu ko'rsatkich 2 281 tani, 2022-yilda esa bir yil avvalgidan ikki baravar, 2 yil avvalgidan 40 baravar ko'payib, 4 332 tani tashkil etgan. Yil davomida qayd etilgan holatlarning 3 372 tasi yoki 82 foizini bank plastik kartalardan pul mablag'larni talon-toroj qilish bilan bog'liq jinoyatlardir. Achinarlisi, axborot texnologiyalari yordamida huquqbuzarlik va jinoyatga qo'l urgan shaxslar orasida yoshlar ko'pchilikni tashkil etmoqda. Respublikamizda virtual olamdagi qonunbuzilishlarning aksariyati 16-23 yosh oralig'idagi o'smir-yoshlar tomonidan sodir qilinmoqda. Bundan ko'rinib turibdiki, kiberxavfsizlikni ta'minlash masalasi bugun har qachongidan ham dolzarb ahamiyat kasb etmoqda.

O‘zbekistonda
2023-yilning 11 oyida 5 ming 5 yuzta kiberjinoyat sodir etildi, shundan 70 foizi bank kartalari bilan bog‘liq firibgarlik va o‘g‘rilik jinoyatlaridir. Tahlillarga ko`ra, dunyo bo`ylab har yili 500 milliondan ortiq kiber hujumlar uyushtiriladi. Har soniyada 12 nafar insondan biri kiber makonda sodir etilgan hujumlar qurboniga aylanadi. Amerika Qo`shma Shtatlari, Fransiya, Angliya, Germaniya, Belgiya, Lyuksemburg kabi rivojlangan davlatlarda jinoyatlarning 60-65 foizi kiber hujumlar orqali sodir etilmoqda.

Hozirda kiberjinoyatchilik borasida AQSh, Rossiya, Korea yetakchi davlatlar qatorida turibdi. Kiberjinoyat tobora yildan yilga ortmoqda bunga asosiy sabab raqamli texnologiyalardir. Hozirda hamma jarayonlar raqamli texnologiyalar asosida bo'layapdi. Masalan olimlarning fikriga qaraganda kiberjinoyatlar yiliga 8-11% gacha o'sar ekan. Kiberjinoyatni sodir etgan shaxslarni topish biroz qiyinroq, chunki o'z ishining ustalari, bir kishi yoki guruh bo'lib ishlashadi. Ularni bu ishga majbur qiladigan narsa bu - pul. Davlat ishida ishlab oylab oylik maoshni kutgandan ko‘ra ular uchun, bitta hakerlik qobilyatini ishga solib qisqa muddatda mo‘maygina mablag‘larni qo'lga kiritishadi.

Smartfoningizdagi shaxsiy ma’lumotlaringizga bo‘lgan tahdidlar. Misol uchun telefonimizdagi suratimizni ijtimoiy tarmoqlardan topib qilinadigan tahdidlar. Bunday holatlar kuzatilmasligi uchun har bir ishimizni nimaga bunday qilayotganimiz haqida o’zimizga savol berib to‘g‘ri anglab, tushunib olishimiz kerak. Shaxsiy ma’lumotlarni og‘irlashda, hammamizni e-mail pochta, id-raqamlar va har xil ma’lumotlarimiz bor ya’ni raqamli ma’lumotlar bular ko‘plab ishimizni bajarib uzoqni yaqin, qiyin jarayonlarni osonlashtiradi. Sizning bu kabi pochtalarga qo’yilgan parolingizni bilib olgan odam deyarli ma’lumot va dars, ish, kundalik hayotingizdagi jarayonlarni nazorat qiladi yoki boshqaradi. Ish xonadagi muhim hujjatlaringizni hamkor chet el davlatlari bilan tuzilgan shartnomalaringizgacha ko‘rib ularni o‘zgartirishi yoki boshqarishi mumkin tizimga qayta kirishingizni cheklab qo‘yishi ham mumkin.

Id-karta, Viza kartalarni boshqarish. Hozirda juda mashhur bo'lgan kiberjinoyatlarning bir turi bank hisob raqamingizdan, virtual kartalaringizdan sizni har xil aldov yo‘li bilan onlayn muloqot tarzida pul undurishi yoki sizni chuv tushurishi mumkin. Bu jarayonlar ustidan ko‘plab arizalar tegishli tartibda Ichki ishlar organlariga kelib tushgan. Bu jarayon juda oson tarzda amalga oshiriladi va siz kiberjinoyat qurboni bo‘lasiz. O‘zingizni har qanday holatda telefon raqamingiz yoki akkauntingizga begona shaxslar, kompaniyalar tomonidan kelgan kodlarni aytmang. Hushyor bo‘ling zamon shiddat bilan rivojlangani bois internet foydalanuvchilari ham ortmoqda. Axborot texnologiyalari aholiga, jamiyatga, davlatga foyda keltiradi va qulaylik yaratadigan dasturlar, platformalar, ilovalar bor. Lekin bular xavfsizlik tomondan hamda boshqa sinovlardan muvaffaqiyatli o‘tganidan keyin ommaga joriy qilgani ma’qul.

O‘zbekistonda kiberjinoyatchilikning oldini olish tizimi yaratiladi. Bu haqda Shavkat Mirziyoyevning “Yangi O‘zbekistonning 2022-2026-yillarga mo‘ljallangan taraqqiyot strategiyasi to‘g‘risida”gi farmoni loyihasida belgilab qo‘yilgan. Qayd etilishicha, 2023-2026-yillar uchun O‘zbekistonning kiberxavfsizlik strategiyasi ishlab chiqiladi. Bunda “uz” domen zonasi internet-makonining kiberxavfsizligini ta’minlashning asosiy yo‘nalishlari belgilanadi. Elektron hukumat, energetika, raqamli iqtisodiyot tizimlari va muhim axborot infratuzilmasiga taalluqli boshqa yo‘nalishlarni himoya qilish bo‘yicha kompleks vazifalar

tuzib chiqiladi. Shuningdek, kiberjinoyatchilik uchun jinoiy javobgarlikni qayta ko‘rib chiqish rejalashtirilgan. Axborot maydonidagi kiberhujum va tahdidlarni monitoring qilish tizimi takomillashtiriladi. Bu orqali kiberxavfsizlik yagona tarmog‘ining texnik infratuzilmasi kengaytiriladi. “Kibernetikada innovatsiyalar IT-parki” faoliyatini yanada jadallashtirish rejalashtirilgan. 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 kiberhujumlar aniqlash bo‘yicha respublika miqyosida konkurslar o‘tkazish nazarda tutilgan.

Kiberjinoyatlarning umumiy profilaktikasining ob’ekti keng jamoatchilikdir va bunda alohida shaxslar tanlab olinmaydi. Masalan, mahalla aholisi, mehnat jamoalari (korxona, muassasa, tashkilotlar), voyaga yetmaganlar jamoasi (maktab, kollej va akademik litseylar), yoshlar jamoasi va boshqalar. Bunda huquqbuzarliklar profilaktikasi barchaga bir xil ravishda yetkazib beriladi va ta’sir doirasi kengroqligi bilan ajralib turadi. Huquqbuzarliklarning umumiy profilaktik faoliyati jamiyatga zid g‘ayriijtimoiy hodisa va jarayonlarning, turli voqea, hodisa va holatlarni aniqlash va ularni bartaraf etish, ta’sir etish, kuchsizlantirish va oldini olishga qaratilgan keng qamrovli ijtimoiy-huquqiy vositalar orqali amalga oshiriladigan faoliyatdir. Aholi orasida huquqiy targ‘ibot ishlarini olib borish huquqbuzarliklarning oldini olishda muhim ahamiyat kasb etadi. Bunda vakolatli organlar tomonidan mehnat, voyaga yetmaganlar kabi jamoalar o‘rtasida Internet tarmoqlaridan foydalanib sodir etiladigan huquqbuzarliklarning oldini olish borasida tushuntirishlar, xususan, ma'ruzalar o‘qish, davra suhbatlari uyushtirish, targ‘ibot bukletlari tayyorlash tarqatish katta samara beradi. Ushbu targ‘ibot tadbirlarida fuqarolarda Internet tarmoqlari orqali sodir etildigan huquqbuzarliklarning salbiy oqibatlari, kelib chiqish sabablari va bu borada shaxslarning xushyorligini oshirish borasida turli vazifalar amalga oshirilishi muhim ahamiyat kasb etadi.

Xulosa qilib aytganda: Kibermakonda sodir etiladigan har bir jinoyatga qarshi kurashish lozim. Bunda Ichki ishlar organlari xodimlarining hissasi katta, chunki yuqorida sanab o’tilgan kiberjinoyatlar yuzasidan nazoratni Kiberxavfsizlik xodimlari amalga oshiradi. Ushbu soha juda keng va chegarasizdir. Kiber xavfsizlikning ichki ishlar organlari tizimidagi o'rni va kiber jinoyatlarni oldini olish mavzusidagi maqolamizning oxirigacha, kiber xavfsizlik muammolari hozirgi zamonning eng muhim muammolaridan biri sifatida o‘z o‘rnini egallaganligi va kiber jinoyatlarining oldini olishning katta ehtiyojiga ega bo‘lishi muhim ahamiyatga ega. Kiber xavfsizlik sohasida faoliyat ko‘rsatuvchi ichki ishlar organlari tizimi, kiber jinoyatlar bilan kurashishda eng muhim qo‘llanmalarimizdan biri hisoblanadi. Bu tizim orqali kiber jinoyatlarini oldini oladigan va fuqarolarni himoya qiladigan tajribali kadrlar tayyorlash, kiber xavfsizlikni oshirish va xavfli tarmoqlarni himoya qilish imkoniyatlarini oshirish uchun katta imkoniyatlar yaratadi. Shuningdek, kiber xavfsizlikning ichki ishlar organlari tizimi, xavfli tarmoqlar va ma'lumotlar bazalarini himoya qilishda katta muhim ahamiyatga ega. Bu tizimning kuchli va samarali bo‘lishi, kiber jinoyatlarini oldini olishda katta rol o‘ynaydi va fuqarolarga xavfli va xavfsiz internet foydalanish imkoniyatlarini ta’minlashda muhim vazifani bajaradi.

Foydalangan adabiyotlar:

1. https://lex.uz/acts/-2387357 “Huqubuzarliklar to‘g‘risida”gi qonun
2. https://lex.uz/uz/docs/-5960604 “Kiberxavfsizlik to‘g‘risida”gi qonun

3. O‘zbekistonda kiberxavfsizlikni ta’minlash – davr talabi tahlil va tavsiyalar.
4. Cyber Security and the Need for International Governance.Charletta Eugenia Anderson-Fortson of Southern University Law Center May 16, 2016.
5. Hasanov Sharofiddin Shamshurovich. Eurasian journal of law, finance and applied sciencesinternational scientific journal special series «outcomes in criminal-procedural relations»
6. https://www.gazeta.uz/oz/tag/kiberxavfsizlik/
7. https://daryo.uz/2022/01/04/ozbekistonning-kiberxavfsizlik-strategiyasi-ishlab-chiqiladi/
8. https://texnokun.uz/?p=7123
9. https://cyberleninka.ru/article/n/kiber-jinoyatlar

INNOVATIVE ACADEMY